RMAT

Análisis y Gestión de Riesgos
Herramientas Adicionales

Ayuda

versión 5.4

15 de enero de 2014

1 ¿Qué hace RMAT? 4
1.1 Primera pantalla 4
1.2 Idiomas 5
1.3 Ficheros: extensiones 6
2 Preparación de perfiles EVL 7
2.1 Consola 7
2.2 Datos del proyecto 8
2.3 Árbol EVL 9
2.3.1 Controles 10
2.3.2 Preguntas 10
2.3.3 Véase también 10
2.3.4 Enlaces 10
2.3.5 Referencias 10
2.3.6 Edición de controles, preguntas y "véase también" 10
2.3.7 Perímetros 12
2.4 Árbol de salvaguardas 13
2.4.1 Salvaguardas 13
2.4.2 Nuevas salvaguardas 13
2.4.3 Nuevo texto para una referencia 13
2.5 EVL edition 13
2.5.1 Menús en la barra superior 14
2.5.2 Botones en la barra superior 16
2.5.3 Botones en la barra inferior 17
..... 17
2.5.4 Cuerpo principal 17
2.5.4.1 [31] En el árbol izquierdo 17
2.5.4.2 [32] Salvaguardas 19
2.6 Información de ayuda 20
2.6.1 Si ROOT es un directorio 20
2.6.2 Si ROOT es un fichero normal … 20
3 Preparación de perfiles sobre perfiles EVL+ 21
3.1 Consola 21
3.2 Datos del proyecto EVL+ 23
3.3 Árbol EVL+ 23
3.3.1 Controles+ 24
3.3.2 Preguntas+ 24
3.3.3 See also 24
3.3.4 Referencias 24
3.3.5 Editar control+, pregunta+, véase también+ 24
3.4 Árbol de controles (derecho) 24
3.4.1 Editar la referencia 24
3.5 Edición Evl+ 24

3.5.1 Botones en la barra superior 25
3.5.2 Botones en la barra superior 26
3.5.3 Botones en la barra inferior 27
3.5.4 Cuerpo principal 28
3.5.4.1 [31] En el árbol izquierdo 28
3.6 Información de ayuda 29
4 Preparación de KB 30
4.1 Consola 30
4.2 Árbol KB 30
4.2.1 Protecciones 31
4.2.2 Editar una protección 31
4.3 Edición del árbol KB 33
5 Preparación de perfiles de amenaza TSV 35
5.1 Consola TSV 35
5.2 Filtros 37
5.3 Identificación 37
5.3.1 columnas 37
5.3.2 clases de activos / amenaza 40
5.3.3 amenazas / clase de activos 41
5.3.4 comparación: clases / clases 42
5.3.5 comparación: amenazas / amenazas 43
5.4 Valoración 45
5.4.1 Amenazas por clase de activos 45
5.4.2 Clases de activos por amenaza 47
5.4.3 Tabla 49
5.5 Consola de pruebas 49
6 Expresiones condicionales para controles y preguntas 51
6.1 Rangos de riesgo 52
6.2 Definición of variables 52
7 Expresiones condicionales para medidas de protección (KB) 53
8 Instalación 54
8.1 Windows 54
8.2 UNIX, Linux 54
8.3 Mac OSX 54

1 ¿Qué hace RMAT?

RMAT ayuda a preparar ficheros para PILAR. Concretamente:

EVL – Security evaluations - Perfiles de seguridad

Correlaciona salvaguardas de PILAR con controles de una norma, pública o privada. Permite un ‘punto de vista’ sobre las medidas de protección del sistema.

Ver *Preparación de perfiles EVL*

EVL+ - Un EVL sobre otro EVL

Un segundo nivel de correlación, construyendo un perfil sobre otro.

Ver *Preparación de perfiles sobre perfiles (EVL+)*

KB – Knowledge databases – Protecciones adicionales

Cuando las salvaguardas estándar son imprecisas, se pueden poner medidas específicas. Típicamente se orienta al servicio de administradores de seguridad que requieren mayor concreción en las medidas a aplicar.

Ver *Preparación de KB*

TSV – Threat standard values – probabilidad y consecuencias de las amenazas sobre los activos

Lo utilizará PILAR para sugerir o aplicar amenazas por defecto, en función de las clases de activos y el valor que deben proteger en cada dimensión de seguridad. Un fichero TSV de alguna forma caracteriza un escenario de ataque.

See *Preparación de perfiles TSV*

1.1 Primera pantalla



1	Fichero de configuración. Haga clic para seleccionar, El fichero de configuración se comparte con PILAR. Ver “Personalización” en la documentación de PILAR para más información.

2	Licencia. Haga clic para seleccionar. Se necesita una licencia válida para ejecutar RMAT.
3	Licencia. Haga clic para seleccionar. Se necesita una licencia válida para ejecutar RMAT.
4	Para editar un perfil de seguridad. Ver *Preparación de perfiles EVL*
5	Para editar un perfil de seguridad basado en otro perfil. Ver *Preparación de perfiles sobre perfiles (EVL+)*
6	Para preparar perfiles de amenazas. Ver *Preparación de perfiles TSV*.
7	Para preparar protecciones adicionales. Ver *Preparación de KB*.
8	Cerrar la aplicación.

1.2 Idiomas

Permite seleccionar varios idiomas para los perfiles de seguridad (EVL) y medidas adicionales (KB). El código de los elementos es único, pero RMAT puede asociarles una descripción en cada idioma.

Un idioma B puede depender de otro A: si no hubiera una descripción en el idioma B, PILAR recurre al texto en idioma A.

La tabla de idiomas muestra todos los idiomas. Las demás pantallas sólo usan el primero de la tabla.



1	idioma	Idioma principal. En las pantallas multi-idioma, habrán entradas para cada uno de los idiomas. El idioma en la primera fila será en el que se use en pantallas con un solo idioma.
2	depende de	Idioma alternativo. Si no se proporciona un texto en el idioma a la izquierda, se recurrirá al texto en el idioma a la derecha.

3	nuevo	Nuevo idioma.
4	arriba	Mueve el idioma seleccionado una fila arriba.
5	abajo	Mueve el idioma seleccionado una fila abajo.
6	eliminar	Elimina la fila: elimina el idioma.
7		Guarda el estado actual del proyecto.
8		OK. Guarda y cierra.
9		CANCELAR. Cierra desechando los datos.

1.3 Ficheros: extensiones

RMAT trabaja con ficheros “fuente” que compila generando ficheros para PILAR.

Los ficheros publicados están cifrados, bien con una contraseña explícita (que se requiere para poder usarlos), o con una contraseña implícita (desde el punto de vista del usuario no hay contraseña).

RMAT usa las siguientes extensiones de ficheros:

herramienta	extensión	descripción
EVL	.tree	la estructura (árbol)
	.lkv	nombres (multi-idioma)
	.evl	publicado para PILAR
EVL+	.vtree	la estructura (árbol)
	.lkv	nombres (multi-idioma)
	.evl	publicado para PILAR
KB	.kbx	la estructura (árbol)
	.kbi	nombres (multi-idioma)
	.kb	publicado para PILAR
TSV	.tsv	XML para PILAR

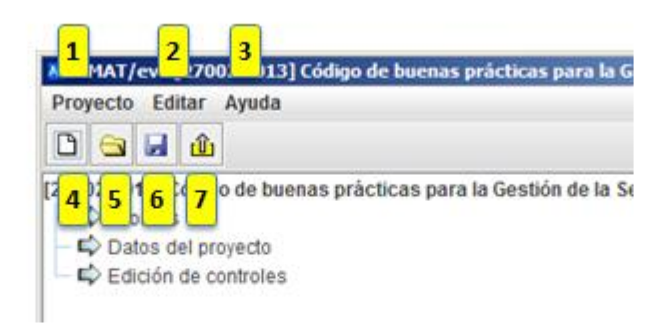
2 Preparación de perfiles EVL

Permite editar un perfil de seguridad EVL que referencia salvaguardas de PILAR.

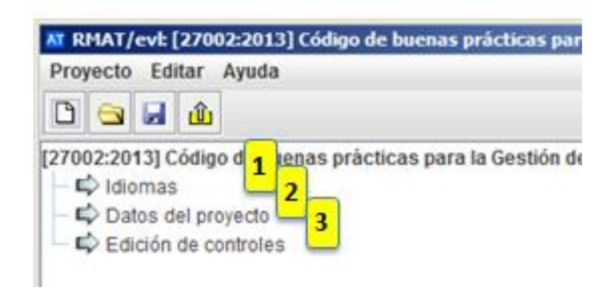
{ evl.controles } → { pilar.salvaguardas }

Para poder usar el perfil EVL en PILAR, es necesario PUBLICARLO usando alguno de los lenguajes disponibles en el perfil y es posible protegerlo con una contraseña.

2.1 Consola

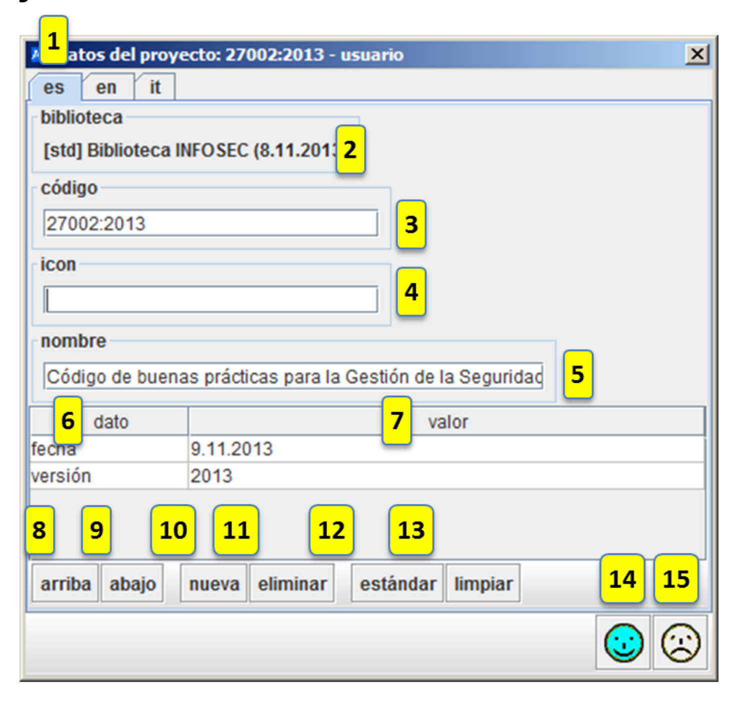


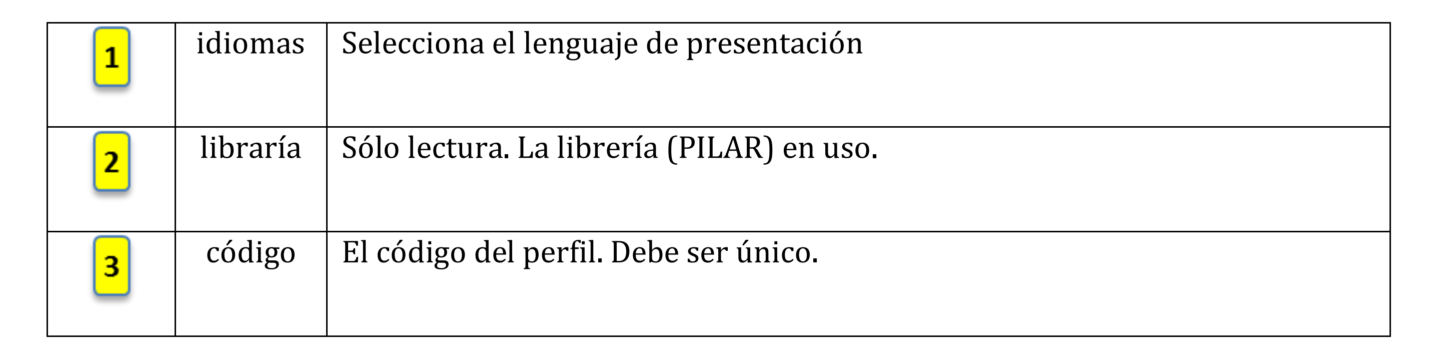
1	Proyecto	Nuevo	Nuevo perfil desde cero
		Abrir	Abre un perfil ya existente (.tree)
		Recientes	Selecciona entre perfiles recientes
		Guardar	Guarda el perfil en su fichero
		Guardar como …	Guarda el perfil en un nuevo fichero
		Publicar	Publica el perfil para que lo use PILAR (.evl)
		Guardar y cerrar	Guarda el perfil en su fichero y cierra
		Cancelar y cerrar	Cierra sin guardar el perfil
2	Editar	Selecciona fuente y tamaño del texto	
3	Ayuda	Presenta la versión en ejecución Chequea actualizaciones	
4		Nuevo perfil desde cero	
5		Abre un perfil ya existente (.tree)	
6		Guarda el perfil en su fichero	
7		Publica el perfil para que lo use PILAR (.evl)	



1	Idiomas	Organiza los diferentes idiomas. Ver *Idiomas*
2	Datos	Datos del proyecto. Ver *Datos del proyecto*
3	Edición	Edición de controles del perfil. Ver *EVL edition*

2.2 Datos del proyecto





1	idiomas	Selecciona el lenguaje de presentación
2	libraría	Sólo lectura. La librería (PILAR) en uso.
3	código	El código del perfil. Debe ser único.

4	icono	Si se indica, se usará con las nuevas salvaguardas.
5	nombre	Meramente descriptivo: el nombre del perfil.
6	dato	Par clave-valor a efectos administrativos
7	valor	Par clave-valor a efectos administrativos
8	arriba	Mueve la fila hacia arriba
9	abajo	Mueve la fila hacia abajo
10	nuevo	Nueva fila
11	eliminar	Elimina la fila seleccionada
12	estándar	Añade claves estándar
13	limpiar	Elimina las filas vacías
14		OK. Guarda el perfil en su fichero y cierra.
15		CANCELAR. Cierra sin guardar el perfil.

2.3 Árbol EVL

Un perfil de seguridad es un árbol de controles.

Los controles pueden refinarse o descomponerse en nuevos controles y preguntas. Controles y preguntas pueden asociarse a salvaguardas.

Usted puede seleccionar uno o más controles y moverlos por el árbol:

MAYÚSCULAS+	**movimiento**
ARRIBA	El nodo se mueve una línea arriba.
ABAJO	El nodo se mueve una línea abajo.
IZQUIERDA	Se desgaja el nodo de sus hermanos y se transforma en un hermano de

	su anterior padre.
DERECHA	Se desgaja el nodo de sus hermanos y se transforma en hijo de su anterior hermano mayor.

2.3.1 Controles

Normalmente se identifican por medio del icono .



Los controles son los elementos principales de un perfil de seguridad.

2.3.2 Preguntas

Normalmente se identifican por medio del icono .

Las preguntas son elementos secundarios, de detalle, dentro de un perfil de seguridad.

2.3.3 Véase también

Icono; .

Sentencias meramente informativas que se intercalan en el perfil de seguridad.

2.3.4 Enlaces

Icono: .

Permiten referenciar un control o pregunta desde otra parte del árbol.

2.3.5 Referencias

Iconos: , según el icono del objeto referido

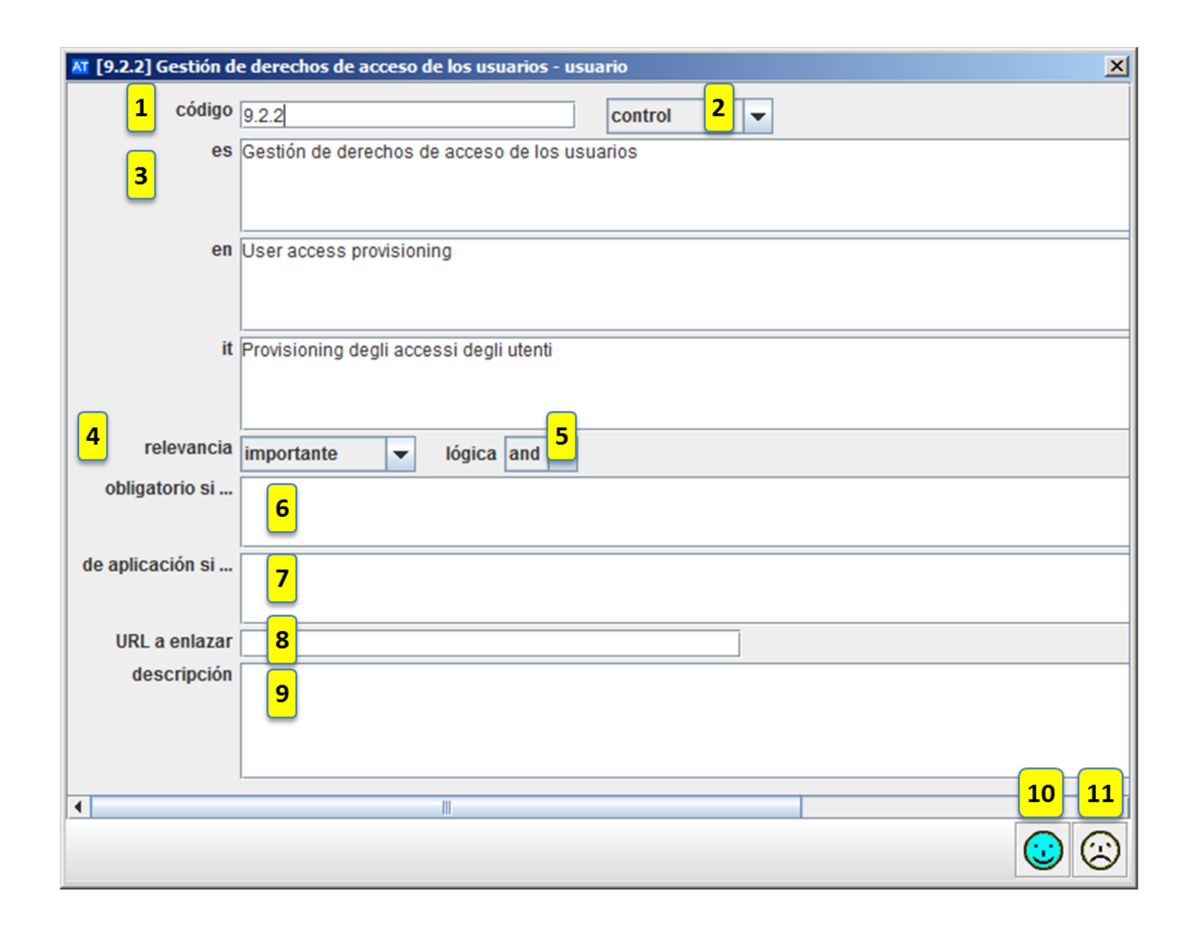
Las referencias son asociaciones desde el perfil de seguridad al árbol de salvaguardas.

Para asociar una [nueva] salvaguarda a un control o una pregunta, hay que arrastrar la salvaguarda desde el panel derecho a su destino en el panel izquierdo.

Para recolocar una referencia, seleccionar y arrastrar con el ratón. También se pueden usar MAYÚSCULAS + FLECHAS.

2.3.6 Edición de controles, preguntas y “véase también”

Se usa una interfaz común para controles, preguntas y “véase también”. De esta forma es sencillo cambiar el papel de un elemento.



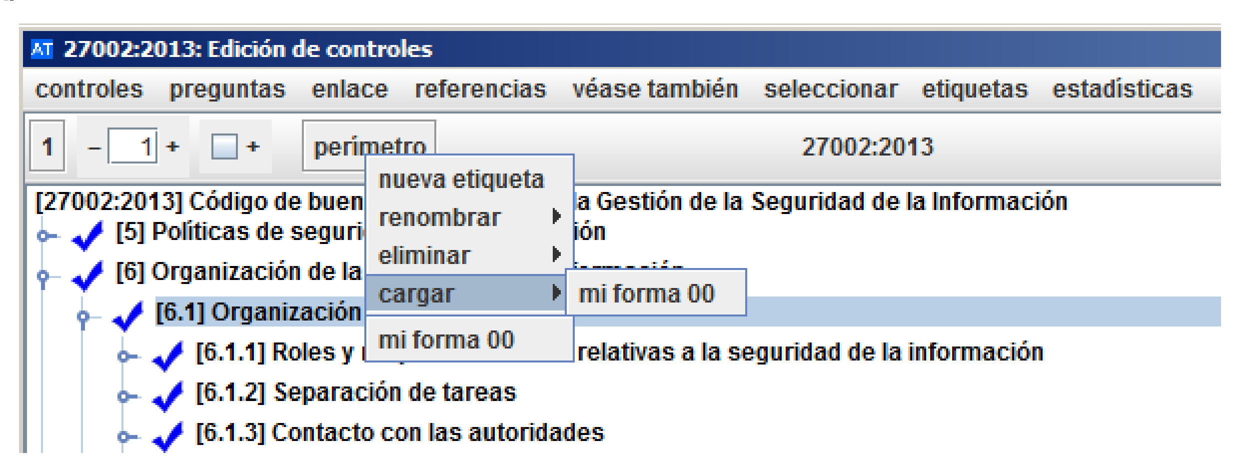
1	código	Un código único. Si es posible, para nuevos controles, RMAT propone un código que es el siguiente en la secuencia numérica o alfabética.
2	clase	Se puede elegir entre “control”, “pregunta” y “véase también”.
3	nombre	Descripción sucinta en cada idioma. Si un nombre está en blanco, PILAR presentará el nombre en el idioma alternativo asociado. Ver *Idiomas*
4	relevancia	Peso relativo del control en su contexto inmediato: crítico: paraguas rojo muy importante: paraguas naranja importante: paraguas verde interesante: paraguas gris
5	lógica	Lógica: cómo se combinan las protecciones en que se descompone AND: todos los hijos cuentan XOR: hay que seleccionar uno de los hijos
6	obligatorio	Ver *Expresiones condicionales*

7	aplica	Ver *Expresiones condicionales*
8	URL	Ver *información de ayuda (EVL)*
9	descripción	Una descripción más larga. Opcional.
10		OK. Guarda el perfil en su fichero y cierra.
11		CANCELAR. Cierra sin guardar el perfil.

2.3.7 Perímetros

Los perímetros son patrones de expansión de árboles. Sirven para darle a un nombre a un determinado nivel de expansión en árboles de salvaguardas y perfiles de seguridad (EVL).

El usuario puede definir perímetros y darles un nombre para ser utilizados posteriormente por PILAR.



Los pasos a seguir son los siguientes:

1. Cree una nueva etiqueta con un nombre de su elección

   `Expandir > perímetro > nueva etiqueta`

2. En el árbol, expanda o contraiga nodos hasta obtener el grado de detalle que le sea útil
3. Cargue el perímetro en su etiqueta

   `Expandir > perímetro > cargar > su etiqueta`

4. Para cambiar el perímetro, repita los pasos 2-3

Par usar una etiqueta

`Expandir > perímetro > su etiqueta`

Para eliminar una etiqueta

`Expandir > perímetro > eliminar > su etiqueta`

2.4 Árbol de salvaguardas

Este árbol se toma prestado de PILAR.

Se puede enriquecer, añadiendo “nuevas salvaguardas”.

Usted puede seleccionar uno o más controles y moverlos por el árbol:

MAYÚSCULAS+	movimiento
ARRIBA	El nodo se mueve una línea arriba.
ABAJO	El nodo se mueve una línea abajo.
IZQUIERDA	Se desgaja el nodo de sus hermanos y se transforma en un hermano de su anterior padre.
DERECHA	Se desgaja el nodo de sus hermanos y se transforma en hijo de su anterior hermano mayor.

2.4.1 Salvaguardas

Las salvaguardas se toman prestadas de PILAR. Tal y como son.

Cuando una salvaguarda es referenciada desde el perfil de seguridad, aún puede editar (modificar) su descripción.

2.4.2 Nuevas salvaguardas

Se denomina nuevas salvaguardas a extensiones del árbol de salvaguardas que se toma de PILAR.

Hay dos formas de añadir salvaguardas:

- Una a una. Haga clic con el botón derecho sobre una salvaguarda para crear e insertar una nueva.
- En bloque: Seleccione un control en el árbol izquierdo. Seleccione una salvaguarda en el árbol derecho. Haga clic con el botón derecho y luego INSERTAR. RMAT busca las hojas (sin hijos) del control, crea una nueva salvaguarda para cada uno de ellos y la referencia desde el control correspondiente.

2.4.3 Nuevo texto para una referencia

La descripción de una salvaguarda puede tener poco sentido

Some safeguards are described with words that only have a meaning in the context of the safeguard tree. When the safeguard is referred to in isolation, the context is lost, and meaning of the safeguard is meaningless. In those situations, you may rephrase (right button) into a new wording. Still, it refers to the same safeguard for evaluation purposes.

Select a reference in the left panel, and right-click to rephrase it.

2.5 EVL edition

Controls are shown on the left panel. Safeguards are on the right panel.

2.5.1 Menús en la barra superior



1	controles	Seleccione la raíz o un control en el panel izquierdo. Haga clic para ... • añadir un nuevo control • editar el control seleccionado • transformar el control en pregunta • eliminar los hijos • eliminar el control y los hijos • sólo mi ruta: cierra todas las ramas del árbol, excepto la que lleva hasta mi • cerrar el padre: cierra las ramas expandidas dejando sólo el nivel de mi padre • cerrar los hermanos: cierra las ramas expandidas dejando sólo el nivel de mis hermanos • cerrar hijos: cierra las ramas expandidas dejando sólo el nivel de mis hijos • visible: si es visible, se publica; si no, no • revisión: control histórico de revisiones
2	preguntas	Seleccione un control o una pregunta en el panel izquierdo. Haga clic para ... • añadir una nueva pregunta • editar la pregunta seleccionada • transformar la pregunta en control • eliminar los hijos • eliminar el control y los hijos • sólo mi ruta: cierra todas las ramas del árbol, excepto la que lleva hasta mi • cerrar el padre: cierra las ramas expandidas dejando sólo el nivel de mi padre • cerrar los hermanos: cierra las ramas expandidas dejando sólo el nivel de mis hermanos • cerrar hijos: cierra las ramas expandidas dejando sólo el nivel de mis hijos • visible: si es visible, se publica; si no, no • revisión: control histórico de revisiones

3	enlace	Un enlace permite referirse a un control o pregunta desde otro lugar Seleccione un control o una pregunta en el panel izquierdo. Haga clic para ... • añadir un nuevo enlace: introduzca el código del objetivo • enlazar al último control seleccionado • editar el enlace • eliminar el enlace
4	referencias	Seleccione una referencia en el panel izquierdo Haga clic para ... • editar: puede proporcionar un texto alternativo; esto es útil cuando la explicación de una salvaguarda pierde su sentido fuera de su contexto en el árbol de salvaguardas • eliminar: se elimina la referencia
5	véase también	Permiten introducir explicaciones textuales.
6	seleccionar	Varios criterios para identificar nodos que satisfacen una cierta condición. En el árbol izquierdo ... • con referencias (enlazados al árbol derecho) • sin referencias (sin enlaces al árbol derecho) • on (visible) pero sin enlaces • off (invisible) pero con enlaces • nuevas salvaguardas (enlaces a nuevas salvaguardas) • revisión abierta En el árbol derecho ... • {0, 0, 0} sin referencias: ni directa, ni indirecta a través de algún ascendiente, ni a ningún descendiente • {*, > 0, *} hay referencias a algún ascendiente • {> 0, > 0, *} hay referencias a mi o a mis ascendientes
7	etiquetas	Se pueden definir etiquetas para agrupar varios nodos bajo un nombre. • nueva etiqueta: crea una nueva etiqueta sin nodos asociados • renombrar: cambio de nombre • eliminar: se elimina la etiqueta • marcar: los nodos seleccionados se asocian a la etiqueta • desmarcar: los nodos seleccionados se disocian de la etiqueta • seleccionar: selecciona los nodos asociados
8	estadísticas	Cuentas • el número de controles • el número de preguntas

		• el número de enlaces • el número de referencias al panel derecho • el número de “véase también”

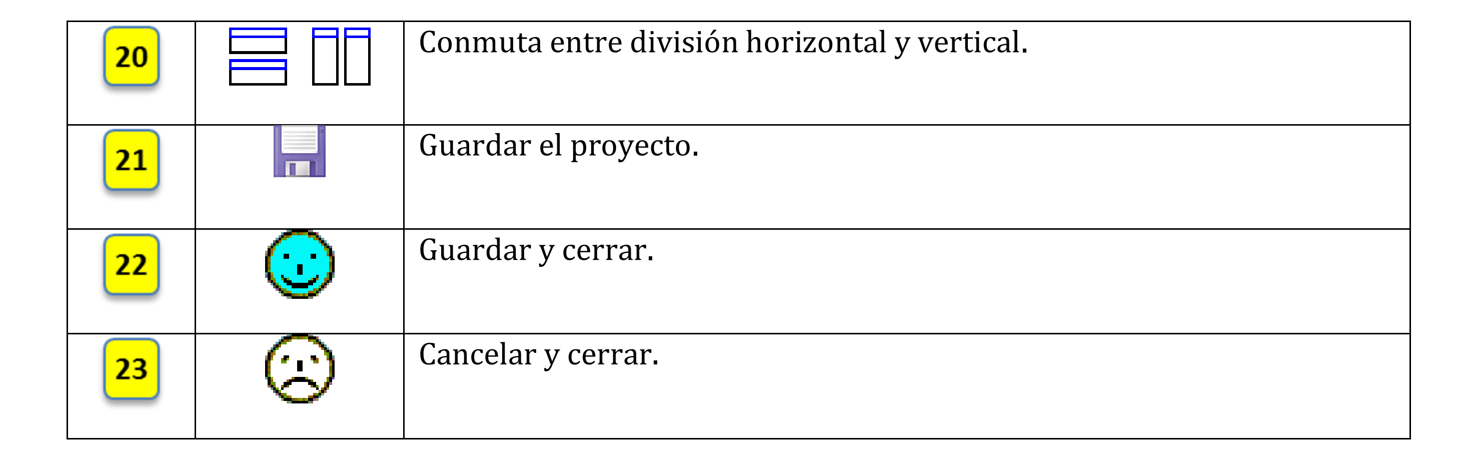
2.5.2 Botones en la barra superior



10	1	Colapsa el árbol izquierdo al primer nivel.
11	– 1 +	Seleccione un control y el nivel de expansión de su sub-árbol.
12	☐ +	Mientras se expande, decide si se expanden las salvaguardas o no.
13	perímetros	Ver “*Perímetros*”.
14	usa …	Seleccione uno o más controles en el panel izquierdo. Haga clic en USA para seleccionar las salvaguardas referenciadas en el panel derecho.
15	1	Colapsa el árbol derecho a nivel 1.
16	– 1 +	Seleccione una salvaguarda y un nivel de expansión de su sub-árbol.
17	usadas	Selecciona las salvaguardas en el árbol derecho que están usadas en algún lugar del árbol izquierdo.
18	usado por	Selecciona los nodos del panel izquierdo desde donde se referencian las salvaguardas del panel derecho.
19	sync	Si hay varios perfiles de seguridad abiertos, si esto está seleccionado, cuando se hace clic en [17], RMAT selecciona los controles relacionados en todos los perfiles.

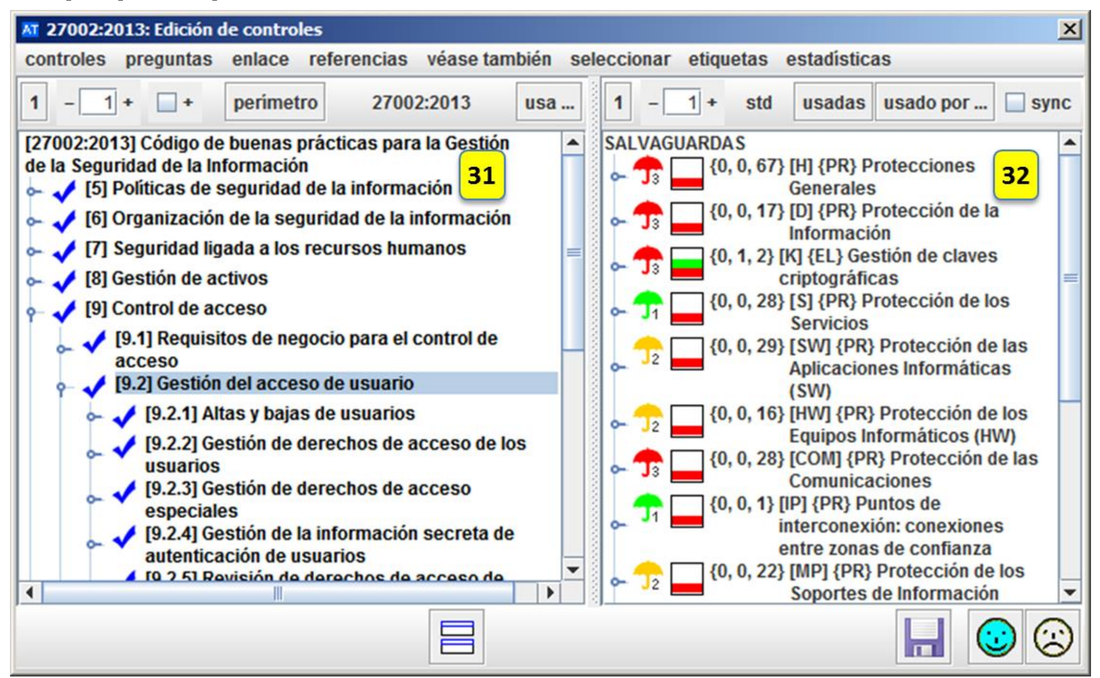
2.5.3 Botones en la barra inferior





20		Conmuta entre división horizontal y vertical.
21		Guardar el proyecto.
22		Guardar y cerrar.
23		Cancelar y cerrar.

2.5.4 Cuerpo principal



2.5.4.1 [31] En el árbol izquierdo

Haga clic en la RAÍZ para …

- editar los datos del perfil de seguridad

Haga clic con el botón derecho en algún CONTROL o PREGUNTA para …

- nuevo
  - nuevo control o pregunta
  - nuevo enlace a otro control o pregunta
  - nuevo enlace al último control o pregunta
  - nuevo “véase también”
- editar el control, o pregunta
- transformar control ← → pregunta
- copiar
- cortar
- pegar
- eliminar los hijos
- eliminar el control o pregunta con sus hijos
- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos
- visible: on para publicar; si no, no se publica
- revisión
  - se puede abrir para revisar
  - se puede cerrar una revisión en curso
  - se puede ver la historia de revisiones abiertas / cerradas

Haga clic con el botón derecho en una REFERENCIA para …

- editar el texto, sustituyendo la descripción original
- eliminar la referencia
- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos

Haga clic con el botón derecho en un ENLACE para …

- editar el enlace
- eliminar el enlace
- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos

Haga clic con el botón derecho en un VÉASE TAMBIÉN para …

- editar el nodo
- eliminar el nodo

- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos

2.5.4.2 [32] Salvaguardas

Las salvaguardas, en el panel derecho muestran el número de referencias desde el panel izquierdo. Se ven 3 números:

{a, m, b}

a número de referencias a elementos por encima; si el valor es mayor que 0, aparece una banda azul en el recuadro:

m número de referencias directas; si el valor es mayor que 0, aparece una banda verde en el recuadro:

b número de referencias a elementos por debajo; si el valor es mayor que 0, aparece una banda roja en el recuadro:

Las cajitas de colores permiten una inspección visual rápida:

AZUL (encima) aparece cuando hay referencias a salvaguardas por encima

VERDE (en medio) aparece cuando hay referencias directas

ROJO (debajo) aparece cuando hay referencias a algún descendiente

... y las bandas van acumulándose: {0, 1, 6};

- 0 referencias por encima
- 1 referencia directa
- 6 referencias por debajo

Haga clic con el botón derecho en una salvaguarda para ...

- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos
- salvaguarda
  - nueva: crea una nueva salvaguardas
  - editar una salvaguarda nueva
  - eliminar una salvaguarda nueva
- control: transforma las hojas no enlazadas bajo los controles seleccionados en salvaguardas nuevas que nacen enlazadas a sus correspondientes en el árbol izquierdo
  - insertar encima
  - insertar dentro (hijo)
  - insertar debajo

2.6 Información de ayuda

Se pueden asociar páginas de ayuda a controles. Por ejemplo, enlaces a la norma que los define.

Sea “xxx” el código del perfil de seguridad. PILAR buscará en el fichero .CAR los siguientes tipos de entradas:

.CAR	anchor
info.xxx = ROOT	define un punto de anclaje para el perfil xxx
info.xxx.C1 = ROOT	define un punto de anclaje para el control C1en el primer nive de xxx.
info.xxx.C1.C2 = ROOT	define un punto de anclaje para el control C2, que es un hijo del control C1, a primer nivel
info.xxx.<path> = ROOT	en general, se puede anclar cualquier control al final de una serie que empieza en el nivel más externo, in general, you may assign the anchor to the final control in a path starting from the top level of profile xxx

El ancla, ROOT, puede ser una ruta absoluta en su sistema de ficheros, o una ruta relativa al directorio HOME que se indica en el fichero de configuración (.car).

2.6.1 Si ROOT es un directorio …

PILAR buscará en el directorio un fichero de nombre “help.map” que asocie códigos a nombres de ficheros.

PILAR analiza el código del control como una serie de nombres separados por puntos. Por ejemplo, sea el control de código “A.B.C”.

1. PILAR busca una asociación para A.B.C en el fichero “help.map”
2. Si hay un fichero F asociado a ese código, PILAR abre ROOT / F
3. Si no hay un fichero asociado, pilar retira el último nombre, quedando “A.B” y seguimos en el punto 1
4. Si nos quedamos sin nombre, PILAR no hace nada

Si no hubiera un fichero “help.map”, PILAR intenta abrir ROOT / A.B.C

2.6.2 Si ROOT es un fichero normal …

PILAR busca el campo URL asociado al control. Si no hay nada, PILAR abre ROOT.

Si hay un URL asociado al control, PILAR lo concatena a ROOT antes de abrirlo.

Ejemplo:

ROOT = Manual.html

url = #subject_3

PILAR abre “HOME / Manual.html #subject_3

3 Preparación de perfiles sobre perfiles EVL⁺

Similar a Preparación de perfiles EVL.

Un EVL establece una correlación:

{ controles del evl } → { salvaguardas de PILAR }

Un EVL⁺ establece una correlación:

{ controles en evl+. } → { controles en evl. }

Para publicar el fichero resultante para PILAR hay que PUBLICAR, eligiendo un idioma y una contraseña opcional.

3.1 Consola



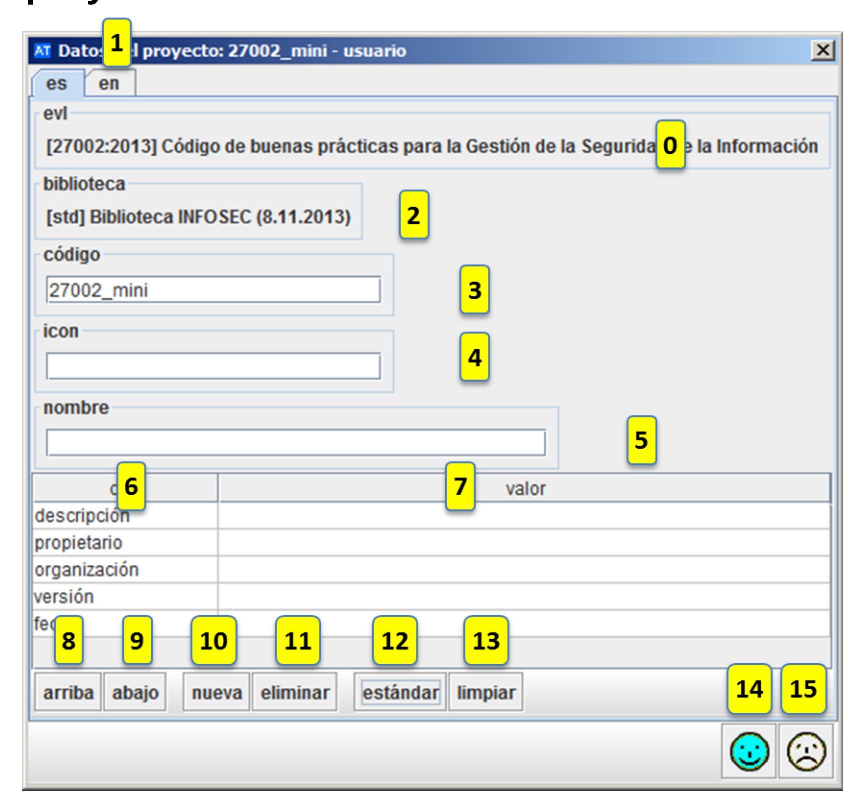
1	Proyecto	Nuevo	Nuevo proyecto, en blanco
		Abrir	Abrir un proyecto ya existente (.vtree)
		Recientes	Volver a abrir un proyecto reciente
		Guardar	Guardar el proyecto
		Guardar como …	Guardar el proyecto con otro nombre
		Publicar	Publicar para PILAR (.evl)
		Guardar y cerrar	Guardar el proyecto y cerrar la ventana
		Cancelar y cerrar	Cancelar los cambios y cerrar la ventana
2	Editar	Ajustar tipo y tamaño de letra	
3	Ayuda	Presenta la versión en ejecución Chequea versiones	
4		Abrir un nuevo proyecto, en blanco	
5		Abrir un proyecto ya existente (.vtree)	

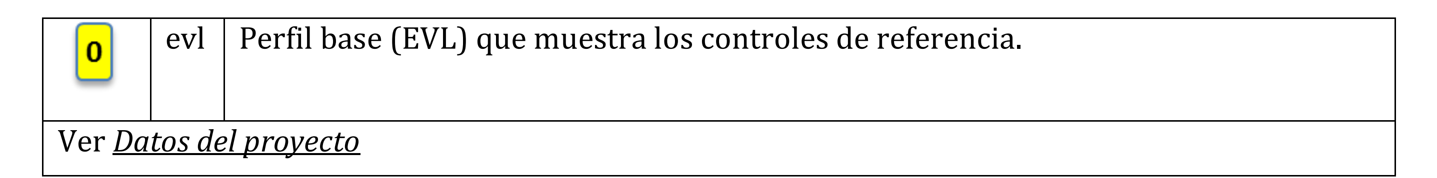
6		Guardar el proyecto
7		Publicar para PILAR (.evl)



1	Idiomas	Organiza los idiomas. Ver *Idiomas*
2	Datos	Edición de los datos del proyecto. Ver *= Datos del proyecto EVL+*
3	Edición	Pantalla de edición de controles. Ver *Edición EVL+*

3.2 Datos del proyecto EVL+





0	evl	Perfil base (EVL) que muestra los controles de referencia.
Ver *Datos del proyecto*		

3.3 Árbol EVL+

EVL+ hace referencia a controles y preguntas en el EVL base.

Puede seleccionar uno o más nodos en el árbol EVL+ y moverlos:

MAYÚSCULAS +	**movement**
ARRIBA	este nodo pasa a la línea superior
ABAJO	este nodo pasa a la línea inferior
IZQUIERDA	el nodo se extrae de sus hermanos y se convierte en el padre de su siguiente hermano
DERECHA	el nodo se extrae de sus hermanos y se convierte en hijo de su hermano mayor

3.3.1 Controles+

Normalmente, con el icono .

Estos controles construyen el marco para organizar referencias al árbol EVL.

3.3.2 Preguntas+

Normalmente, con el icono .

Las preguntas son elementos secundarios, de detalle, dentro del perfil de seguridad.

3.3.3 See also

Icono .

Elementos informativos empotrados en el perfil.

3.3.4 Referencias

Las referencias apuntan a elementos del árbol EVL base. En icono es el del elemento referenciado.

Para asociar un control+ o una pregunta+ a un elemento del árbol EVL, use el ratón para seleccionar y arrastrar desde el panel derecho al izquierdo. Para cambiar una referencia de sitio: seleccionar y arrastrar, o bien usar MAYÚSCULAS + FLECHA.

3.3.5 Editar control+, pregunta+, véase también+

Ver *Edición de controles*

3.4 Árbol de controles (derecho)

Este árbol se importa del perfil EVL.

3.4.1 Editar la referencia

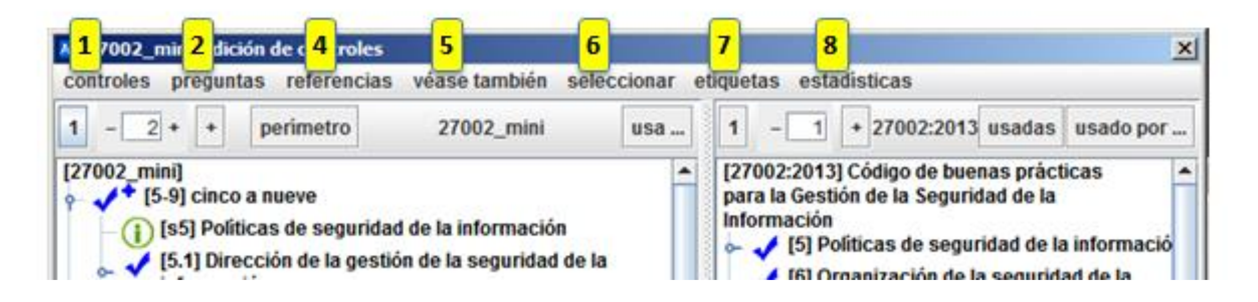
Algunos elementos están descritos con palabras que sólo tienen sentido en el contexto del árbol y cuando se extraen del contexto quedan incomprensibles. En estas circunstancias puede proporcionar un texto alternativo para ver el control en su nuevo contexto.

Seleccione una referencia en el panel izquierdo para editarla.

3.5 Edición Evl+

Los nuevos controles ( ) se muestran en el árbol izquierdo. Los controles importados ( ) aparecen en el árbol derecho.

3.5.1 Botones en la barra superior



1	controles	Seleccione la raíz o un control en el panel izquierdo. Haga clic para ... • añadir un nuevo control • editar el control seleccionado • transformar el control en pregunta • eliminar los hijos • eliminar el control y los hijos • sólo mi ruta: cierra todas las ramas del árbol, excepto la que lleva hasta mi • cerrar el padre: cierra las ramas expandidas dejando sólo el nivel de mi padre • cerrar los hermanos: cierra las ramas expandidas dejando sólo el nivel de mis hermanos • cerrar hijos: cierra las ramas expandidas dejando sólo el nivel de mis hijos • visible: si es visible, se publica; si no, no • revisión: control histórico de revisiones
2	preguntas	Seleccione un control o una pregunta en el panel izquierdo. Haga clic para ... • añadir una nueva pregunta • editar la pregunta seleccionada • transformar la pregunta en control • eliminar los hijos • eliminar el control y los hijos • sólo mi ruta: cierra todas las ramas del árbol, excepto la que lleva hasta mi • cerrar el padre: cierra las ramas expandidas dejando sólo el nivel de mi padre • cerrar los hermanos: cierra las ramas expandidas dejando sólo el nivel de mis hermanos • cerrar hijos: cierra las ramas expandidas dejando sólo el nivel de mis hijos • visible: si es visible, se publica; si no, no • revisión: control histórico de revisiones

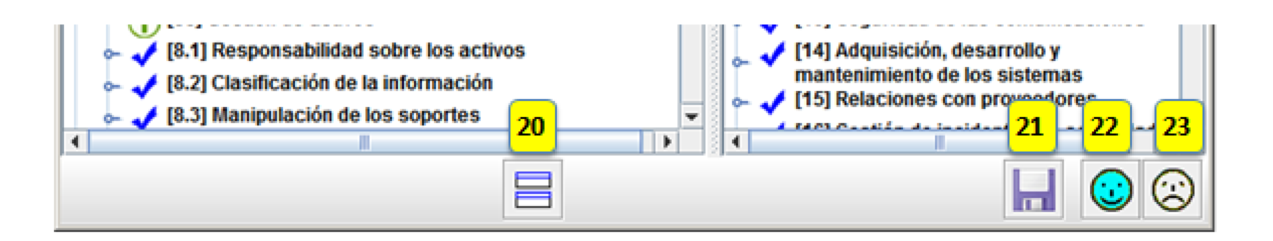
4	referencias	Seleccione una referencia en el panel izquierdo Haga clic para … • editar: puede proporcionar un texto alternativo; esto es útil cuando la explicación de una salvaguarda pierde su sentido fuera de su contexto en el árbol de salvaguardas • eliminar: se elimina la referencia
5	véase también	Permiten introducir explicaciones textuales.
6	seleccionar	Varios criterios para identificar nodos que satisfacen una cierta condición. En el árbol izquierdo … • con referencias (enlazados al árbol derecho) • sin referencias (sin enlaces al árbol derecho) • on (visible) pero sin enlaces • off (invisible) pero con enlaces • revisión abierta
7	etiquetas	Se pueden definir etiquetas para agrupar varios nodos bajo un nombre. • nueva etiqueta: crea una nueva etiqueta sin nodos asociados • renombrar: cambio de nombre • eliminar: se elimina la etiqueta • marcar: los nodos seleccionados se asocian a la etiqueta • desmarcar: los nodos seleccionados se disocian de la etiqueta • seleccionar: selecciona los nodos asociados
8	estadísticas	Cuentas • el número de controles • el número de preguntas • el número de referencias al panel derecho • el número de “véase también”

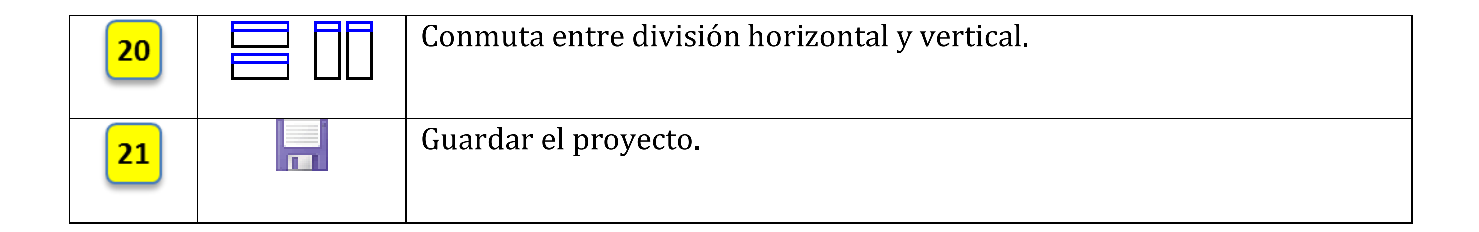
3.5.2 Botones en la barra superior



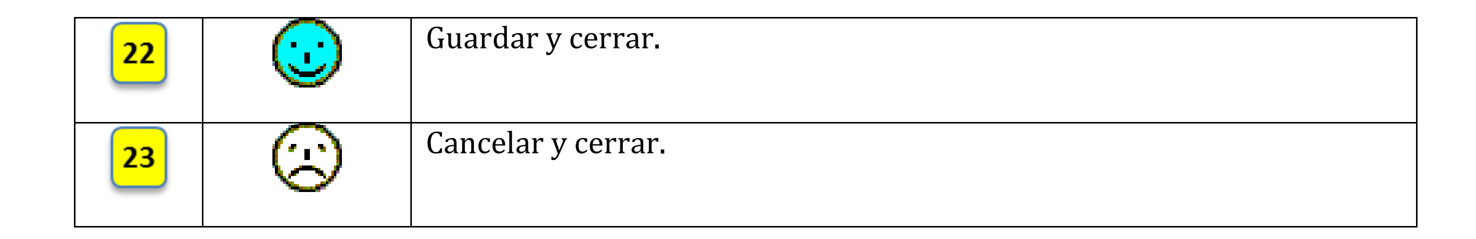
10	1	Colapsa el árbol izquierdo al primer nivel.
11	– 1 +	Seleccione un control y el nivel de expansión de su sub-árbol.
12	☐ +	Reservado para uso futuro.
13	perímetros	Ver "*Perímetros*".
14	usa ...	Seleccione uno o más controles en el panel izquierdo. Haga clic en USA para seleccionar los elementos referenciados en el panel derecho.
15	1	Colapsa el árbol derecho a nivel 1.
16	– 1 +	Seleccione un control y un nivel de expansión de su sub-árbol.
17	+1	Si no está seleccionado, la expansión [16] para cuando no hay más controles. Si se selecciona, la expansión continua con las salvaguardas referenciadas.
18	usadas	Selecciona los controles en el árbol derecho que están usados en algún lugar del árbol izquierdo.
19	usado por	Selecciona los nodos del panel izquierdo desde donde se referencian elementos del panel derecho.

3.5.3 Botones en la barra inferior



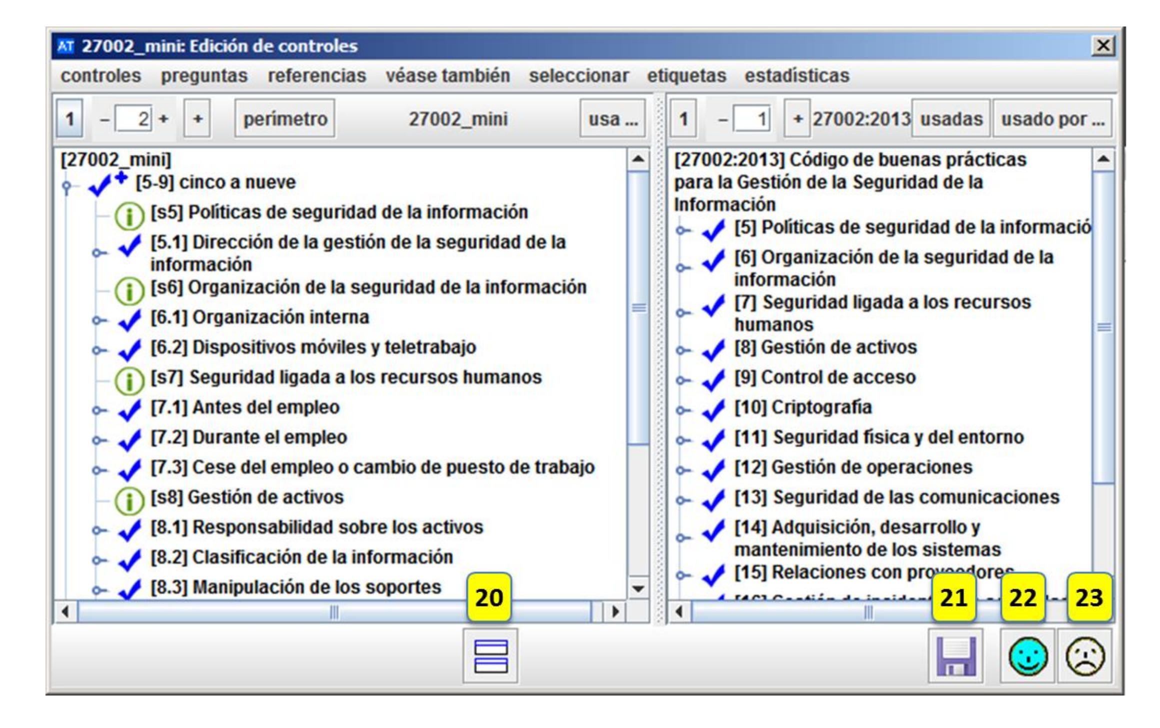


20		Conmuta entre división horizontal y vertical.
21		Guardar el proyecto.



22		Guardar y cerrar.
23		Cancelar y cerrar.

3.5.4 Cuerpo principal



3.5.4.1 [31] En el árbol izquierdo

Haga clic en la RAÍZ para ...

- editar los datos del perfil de seguridad

Haga clic con el botón derecho en algún CONTROL+ o PREGUNTA+ para ...

- nuevo
  - nuevo control+ o pregunta+
  - nuevo "véase también"
- editar el control+ o pregunta+
- transformar control+ ← → pregunta+
- copiar
- cortar
- pegar
- eliminar los hijos
- eliminar el control+ o pregunta+ con sus hijos
- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos

- cerrar mis hijos
- visible: on para publicar; si no, no se publica
- revisión
    - se puede abrir para revisar
    - se puede cerrar una revisión en curso
    - se puede ver la historia de revisiones abiertas / cerradas

Haga clic con el botón derecho en una REFERENCIA para …

- editar el texto, sustituyendo la descripción original
- eliminar la referencia
- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos

Haga clic con el botón derecho en un VÉASE TAMBIÉN para …

- editar el nodo
- eliminar el nodo
- sólo mi ruta: colapsa todas las ramas del árbol excepto el camino que lleva al nodo seleccionado.
- cerrar el padre
- cerrar mis hermanos
- cerrar mis hijos

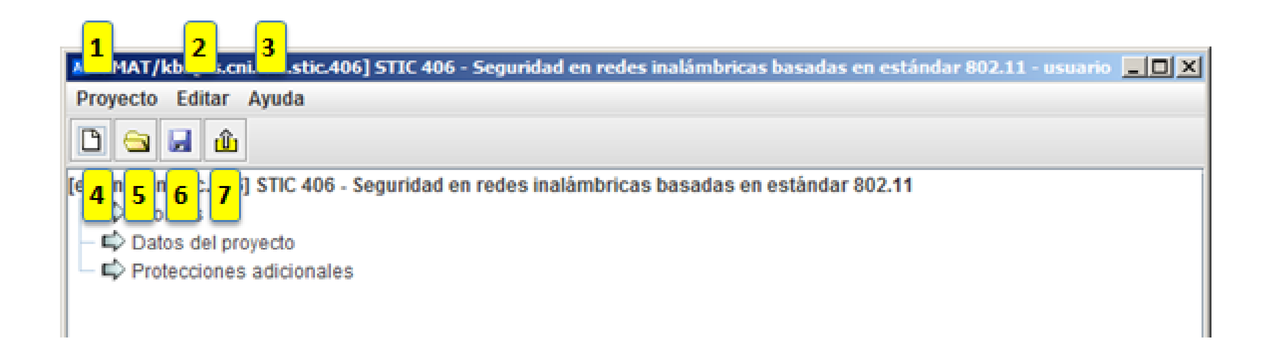
3.6 Información de ayuda

Ver *información de ayuda (EVL)*

4 Preparación de KB

Esta funcionalidad permite editar y publicar protecciones adicionales para activos.

4.1 Consola



1	Proyecto	Nuevo	Nuevo proyecto, en blanco
		Abrir	Abrir un proyecto ya existente (.kbx + .kbi)
		Recientes	Volver a abrir un proyecto reciente
		Guardar	Guardar el proyecto
		Guardar como …	Guardar el proyecto con otro nombre
		Publicar	Publicar para PILAR (.kb)
		Guardar y cerrar	Guardar el proyecto y cerrar la ventana
		Cancelar y cerrar	Cancelar los cambios y cerrar la ventana
2	Editar	Ajustar tipo y tamaño de letra	
3	Ayuda	Presenta la versión en ejecución Chequea versiones	
4		Abrir un nuevo proyecto, en blanco	
5		Abrir un proyecto ya existente (.kbx)	
6		Guardar el proyecto	
7		Publicar para PILAR (.kb)	

4.2 Árbol KB

Un árbol de protecciones.

Las protecciones pueden detallarse con sub-árboles.

Puede seleccionar uno más nodos del árbol KB y moverlos dentro del árbol:

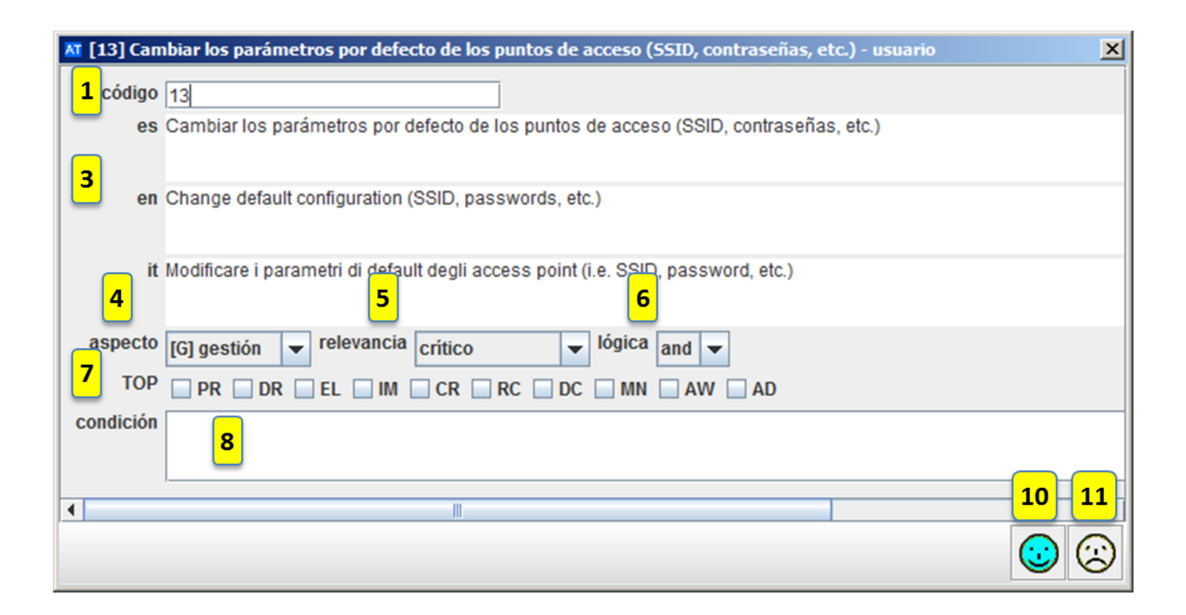
MAYÚSCULAS+	movimiento
ARRIBA	El nodo se mueve una línea arriba.
ABAJO	El nodo se mueve una línea abajo.
IZQUIERDA	Se desgaja el nodo de sus hermanos y se transforma en un hermano de su anterior padre.
DERECHA	Se desgaja el nodo de sus hermanos y se transforma en hijo de su anterior hermano mayor.

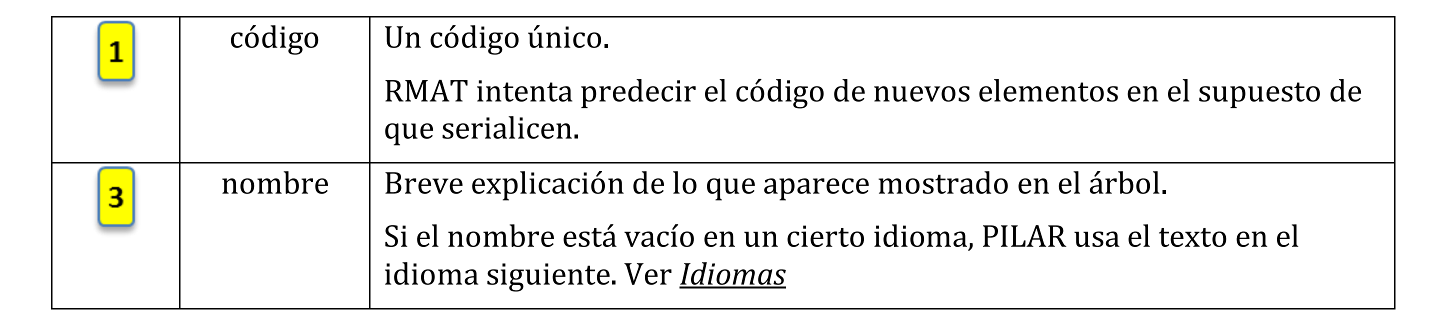
4.2.1 Protecciones

Normalmente, se usan los iconos  or .

Las protecciones son elementos del árbol de protecciones.

4.2.2 Editar una protección

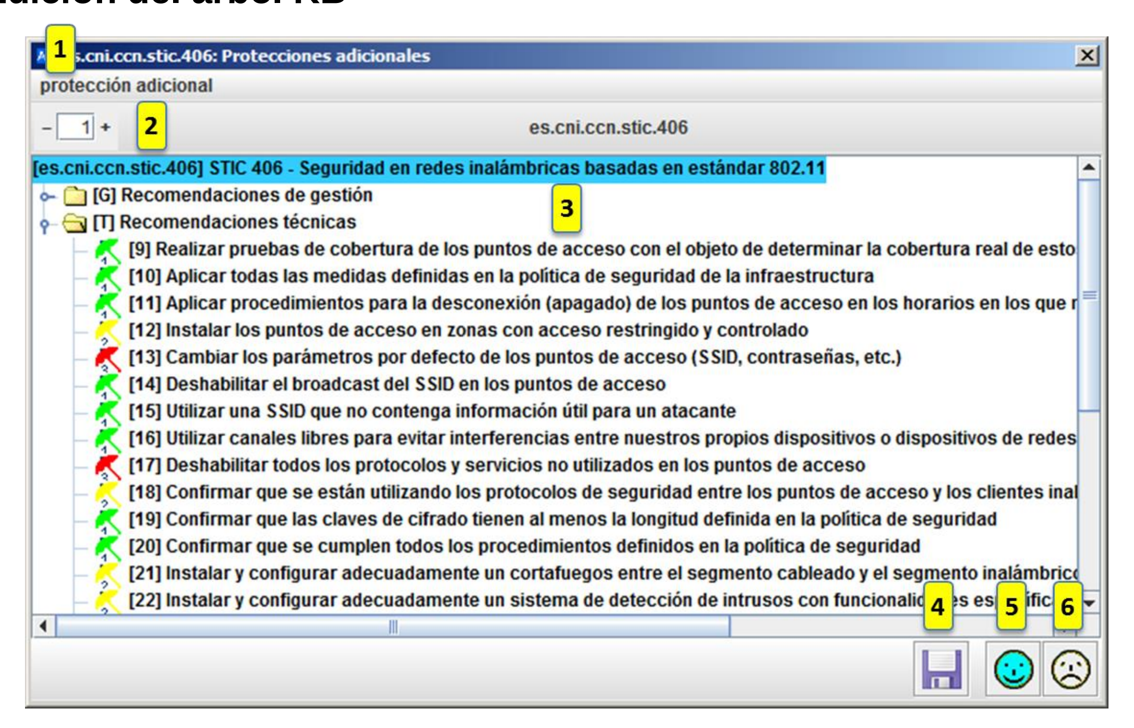




1	código	Un código único. RMAT intenta predecir el código de nuevos elementos en el supuesto de que serialicen.
3	nombre	Breve explicación de lo que aparece mostrado en el árbol. Si el nombre está vacío en un cierto idioma, PILAR usa el texto en el idioma siguiente. Ver *Idiomas*

4	aspecto	G Medida de gestión T Medida técnica F Seguridad física P Gestión del personal
5	relevancia	Peso relativo del elemento en su entorno más inmediato: 3 crítico: paraguas rojo 2 muy importante: paraguas amarillo 1 importante: paraguas verde 0 interesante: paraguas gris
6	lógica	¿Cómo combinan los elementos inferiores de detalle? AND: todos los hijos cuentan XOR: hay que seleccionar uno de los hijos
7	TDP	Tipo de protección PR – preventiva DR – disuasoria EL – se elimina el problema IM – se minimiza el impacto CR – correctiva RC – medidas de recuperación DC – detección MN – monitorización AW – concienciación AD – medidas administrativas
8	condición	Ver *Expresiones condicionales*
10		OK. Guardar y cerrar.
11		CANCELAR. Desechar y cerrar.

4.3 Edición del árbol KB



1	protección adicional 0 1 2 3	Seleccione la raíz o un control del árbol Haga clic para ... • añadir una nueva protección • editar una protección • eliminar los hijos • eliminar la protección junto con sus hijos • sólo mi ruta: cierra todas las ramas del árbol, excepto la que lleva hasta mi • cerrar el padre: cierra las ramas expandidas dejando sólo el nivel de mi padre • cerrar los hermanos: cierra las ramas expandidas dejando sólo el nivel de mis hermanos • cerrar hijos: cierra las ramas expandidas dejando sólo el nivel de mis hijos • visible: si es visible, se publica; si no, no
2	- 1 +	Seleccione una protección y el nivel de expansión de su sub-árbol.
3		Arbol de protecciones
4		Guardar el proyecto.
5		Guardar y cerrar.

6		Cancelar y cerrar.

5 Preparación de perfiles de amenaza TSV

Esta funcionalidad se utiliza para preparar ficheros .TSV (Threat Standard Values)

El formato de los ficheros TSV es como sigue:

```
fichero ::=
    <threat-standard-values>
      { family }0+
    </threat-standard-values>

family ::=
    <family F >
       { threat }0+
    </family>

threat ::=
    <threat Z f [ s ] >
      { set }0+
    </threat>

set ::=
    <set D deg />
```

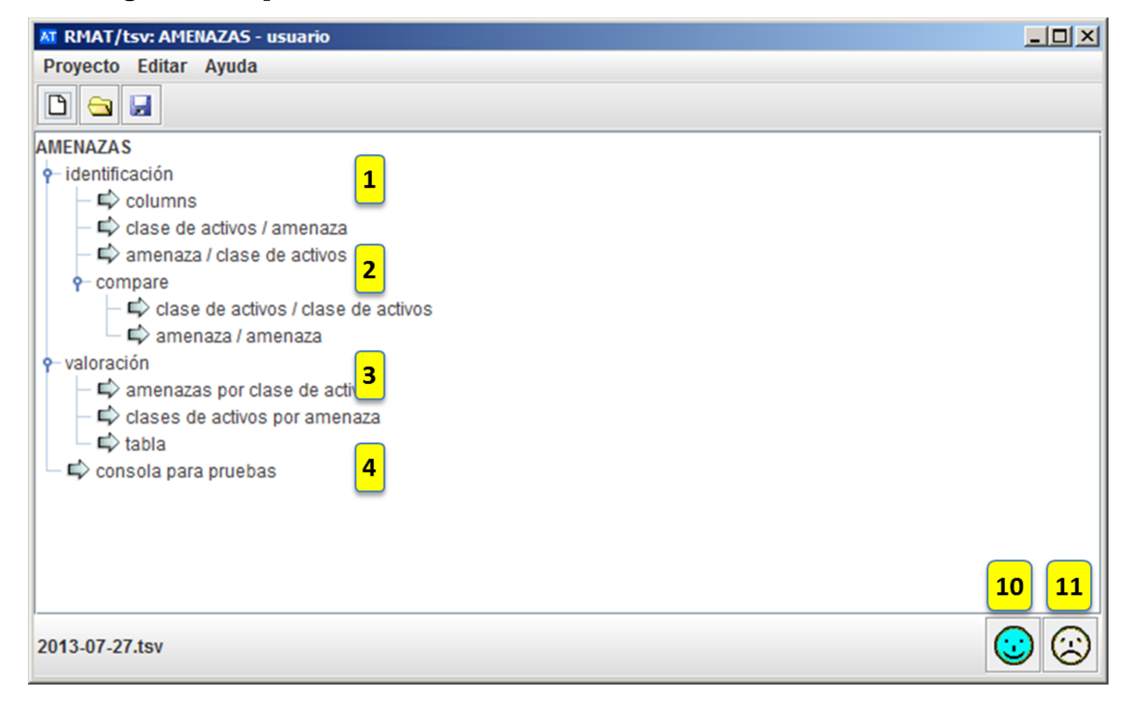
attributes	
F	el código de una familia (clase de activos)
Z	el código de una amenaza
f	la frecuencia (esperada) de la amenaza número real >= 0,0
s	el intervalo esparado de interrupción de la disponibilidad como consecuencia de la amenaza
D	el código de una dimensión de seguridad
deg	la degradación causada por la amenaza número real entre 0.0 y 1.0

5.1 Consola TSV



1	Proyecto	Nuevo	Nuevo perfil desde cero
		Abrir	Abre un perfil ya existente (.tsv)
		Recientes	Selecciona entre perfiles recientes
		Guardar	Guarda el perfil en su fichero
		Guardar como …	Guarda el perfil en un nuevo fichero
		Guardar y cerrar	Guarda el perfil en su fichero y cierra
		Cancelar y cerrar	Cierra sin guardar el perfil
2	Editar	Selecciona fuente y tamaño del texto	
3	Ayuda	Presenta la versión en ejecución Chequea actualizaciones	
4		Nuevo perfil desde cero	
5		Abre un perfil ya existente (.tsv)	
6		Guarda el perfil en su fichero	

Se ofrecen las siguientes opciones:

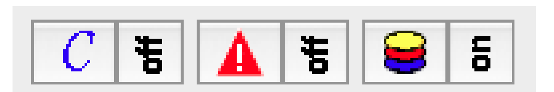


- [1] identificación:
  para asociar amenazas a clases de activos
    - por columnas

        - clases de activo por amenaza
        - amenazas por clase de activo
        - [2] compara
            - clases / clases
            - amenazas / amenazas
- [3] valoración
    - amenazas por clase de activo:
      para asignar valores de probabilidad (frecuencia) y de degradación a cada amenaza para cada clase de activo
    - clases de activo por amenaza
      para asignar valores de probabilidad (frecuencia) y de degradación a cada clase de activo para cada amenaza
    - tabla:
      presentación plana de clases de activos, amenazas, probabilidades y degradaciones
- [4] consola de pruebas:
  permite seleccionar una clase de activos, o una combinación de clases y ver qué amenazas les asignaría PILAR

5.2 Filtros

Puede imponer filtro sobre las clases de activos, amenazas y dimensiones. Cuando se activa un filtro, RMAT sólo presenta los valores seleccionados.



La selección puede hacerse en cualquiera de las pantallas de amenazas, y se conserva hasta que se cierra la edición.

Los elementos se presentan como árboles. Haga clic en un elemento para conmutas su visibilidad: ON / OFF

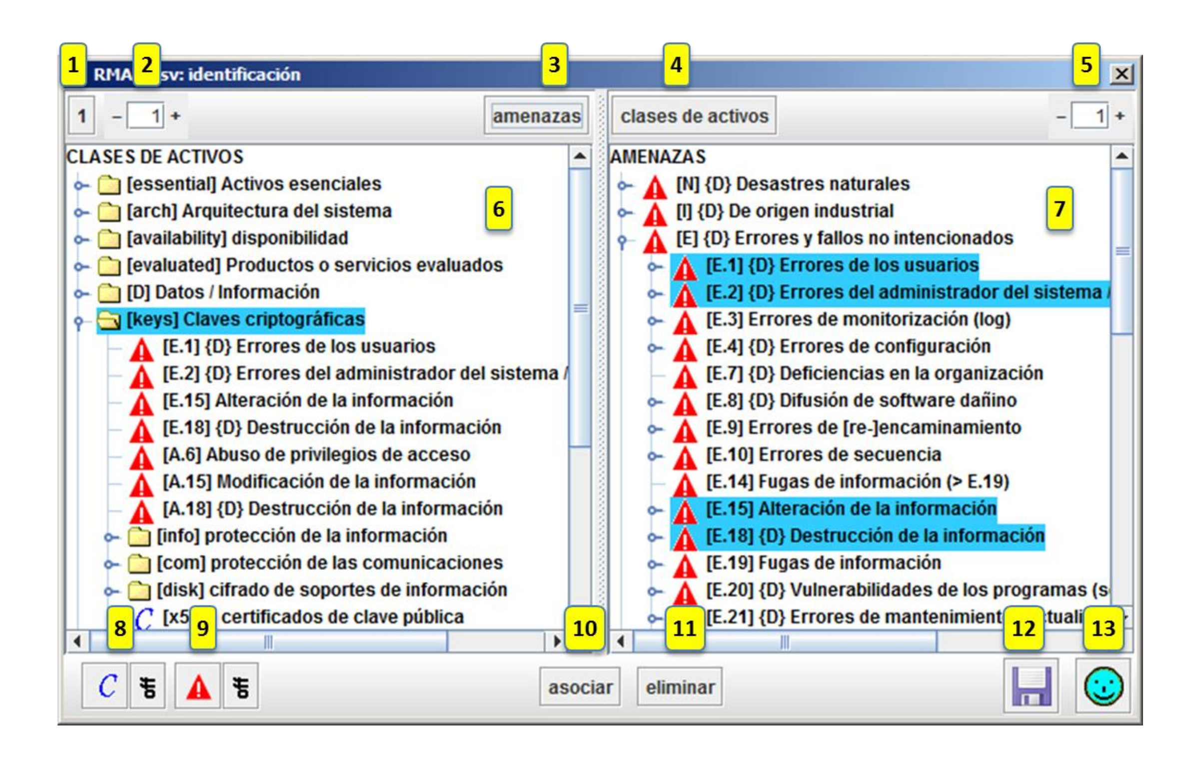
5.3 Identificación

5.3.1 columnas

Para asociar amenazas a clases de activos.

El panel izquierdo muestra las clases de activos y las amenazas asociadas.

El panel derecho muestra las amenazas y las clases de activos asociadas .



1	1	Colapsa el árbol izquierdo al primer nivel.
2	– 1 +	Seleccione un control y el nivel de expansión de su sub-árbol.
3	amenazas	Seleccione un activo en el árbol izquierdo [6], haga clic en [3] y RMAT seleccionará las amenazas asociadas en l panel derecho [7].
4	clases de activos	Seleccione una amenaza en el árbol derecho [7], haga clic en [4] y RMAT seleccionará las clases de activos asociadas en l panel derecho [7].
5	– 1 +	Seleccione un nodo en el árbol derecho [7], y el nivel de expansión de su sub-árbol
6		Árbol de clases de activos y las amenazas asociadas.
7		Árbol de amenazas con sus clases de activos asociadas.
8	C	Filtro de clases de activos. Haga clic para seleccionar qué activos quiere ver.
9		Filtro de amenazas. Haga clic para seleccionar qué amenazas quiere ver.
10	asociar	Seleccione una o más clases en el árbol izquierdo [6], y una o más amenazas en el árbol derecho [7]. Haga clic en [10] para asociar las amenazas a la clase de activos.

11	eliminar	Seleccione una o más amenazas en el árbol izquierdo [6] y haga clic en [11] para eliminarlas. Seleccione una o más clases en el árbol izquierdo [6], y una o más amenazas en el árbol derecho [7]. Haga clic en [11] para eliminar la asociación.
12		Guardar el proyecto.
13		Guardar y cerrar.

Para seleccionar las amenazas asociadas a una clase de activos,

1. seleccione una o más clases a la izquierda
2. haga clic en AMENAZAS (arriba)
3. las amenazas asociadas aparecen seleccionadas a la derecha

Para seleccionar las clases asociadas a una amenaza,

1. seleccione una o más amenazas a la derecha
2. haga clic en ACTIVOS (arriba)
3. las clases asociadas aparecen seleccionadas a la derecha

Para encontrar una clase de activos,

1. enfoque el árbol izquierdo
2. CTRL+F

Para encontrar una amenaza

1. enfoque el árbol derecho
2. CTRL+F

Para asociar una amenaza a una clase de activos,

1. seleccione una o más familias a la izquierda
2. seleccione una o más amenazas a la derecha
3. haga clic en ASOCIAR

Para disociar una amenaza de una clase de activos,

1. seleccione una o más clases a la izquierda
2. seleccione una o más amenazas a la derecha
3. haga clic en ELIMINAR

o

1. expanda el árbol izquierdo hasta que aparezca la amenaza que desea eliminar
2. seleccione la amenaza a eliminar
3. haga clic en ELIMINAR

o

1. expanda el árbol derecho hasta que aparezca la clase que desea eliminar
2. seleccione la clase a eliminar
3. haga clic en ELIMINAR

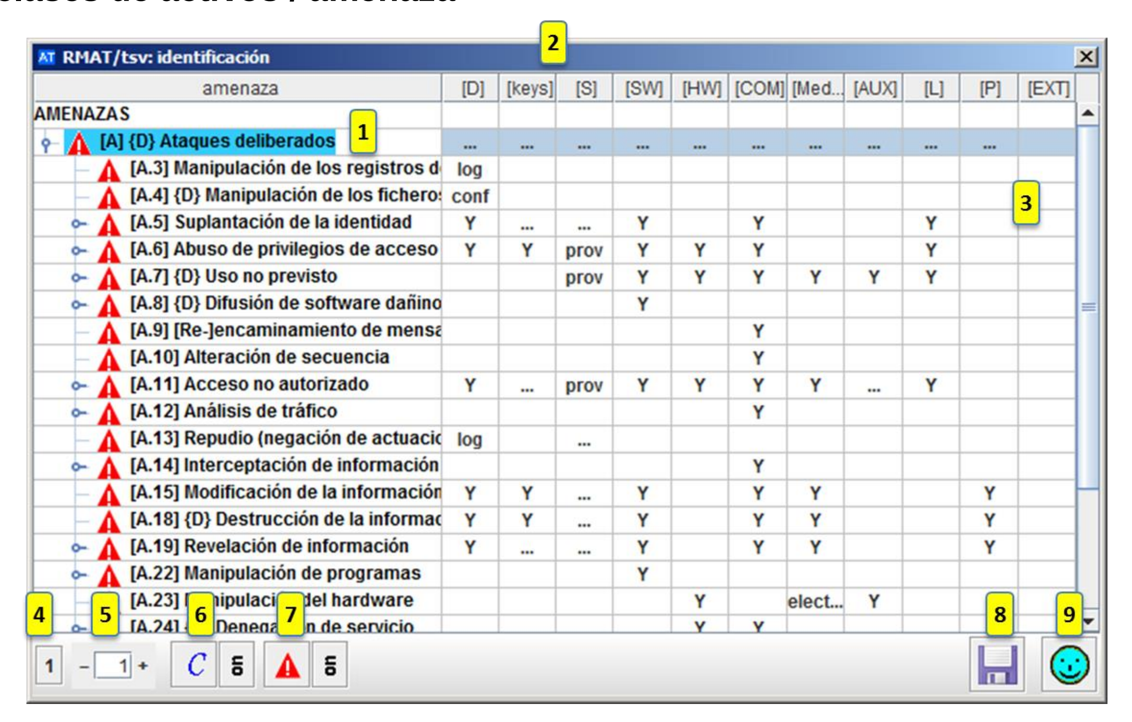
Para salvar los datos actuales,

1. haga clic en GUARDAR

Para guardar los cambios y salir,

1. haga clic en OK

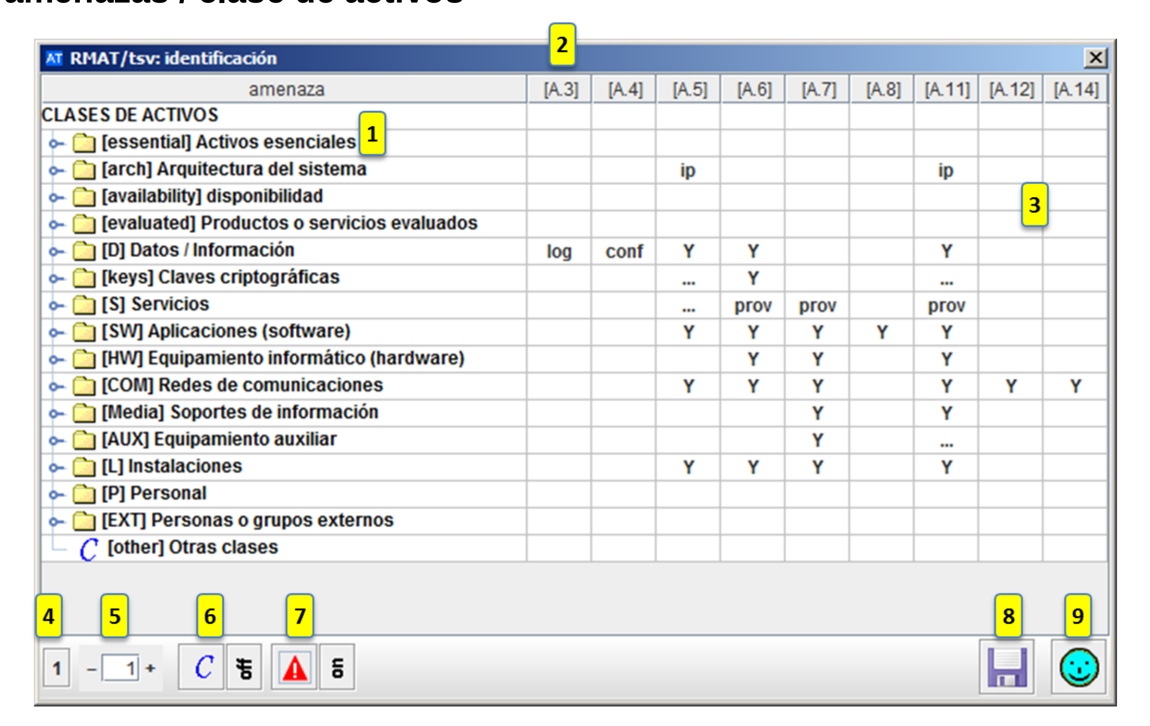
5.3.2 clases de activos / amenaza



1		Árbol de amenazas. Use el filtro [7] para acotar lo que se ve.
2		Clases de activos. Use el filtro [6] para acotar lo que se ve.
3		Relación entre las clases de activos [2] y las amenazas [1] en blanco — sin relación Y — relacionadas ... — expandir para ver los detalles clase — sólo asociada a la clase indicada
4	1	Relación entre las clases de activos [2] y las amenazas [1] en blanco — sin relación Y — relacionadas ... — expandir para ver los detalles clase — sólo asociada a la clase indicada

5	- 1 +	Seleccione un nodo en [1], y seleccione un nivel de expansión de su sub-árbol.
6		Filtro para clases de activos. Haga clic para seleccionar lo que quiere ver..
7		Filtro para amenazas. Haga clic para seleccionar lo que quiere ver..
8		Guardar el proyecto.
9		Guardar y cerrar.

5.3.3 amenazas / clase de activos



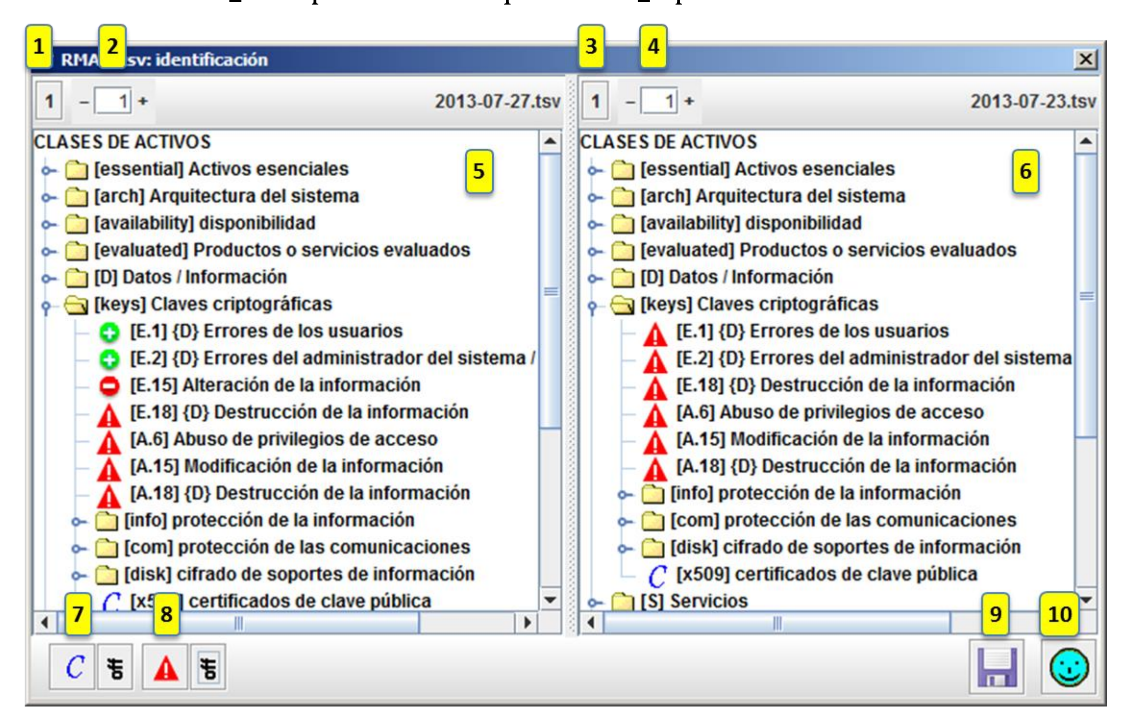
amenaza	[A.3]	[A.4]	[A.5]	[A.6]	[A.7]	[A.8]	[A.11]	[A.12]	[A.14]
CLASES DE ACTIVOS									
[essential] Activos esenciales									
[arch] Arquitectura del sistema			ip				ip		
[availability] disponibilidad									
[evaluated] Productos o servicios evaluados									
[D] Datos / Información	log	conf	Y	Y			Y		
[keys] Claves criptográficas			...	Y			...		
[S] Servicios			...	prov	prov		prov		
[SW] Aplicaciones (software)			Y	Y	Y	Y	Y		
[HW] Equipamiento informático (hardware)				Y	Y		Y		
[COM] Redes de comunicaciones			Y	Y	Y		Y	Y	Y
[Media] Soportes de información					Y		Y		
[AUX] Equipamiento auxiliar					Y		...		
[L] Instalaciones			Y	Y	Y		Y		
[P] Personal									
[EXT] Personas o grupos externos									
[other] Otras clases									

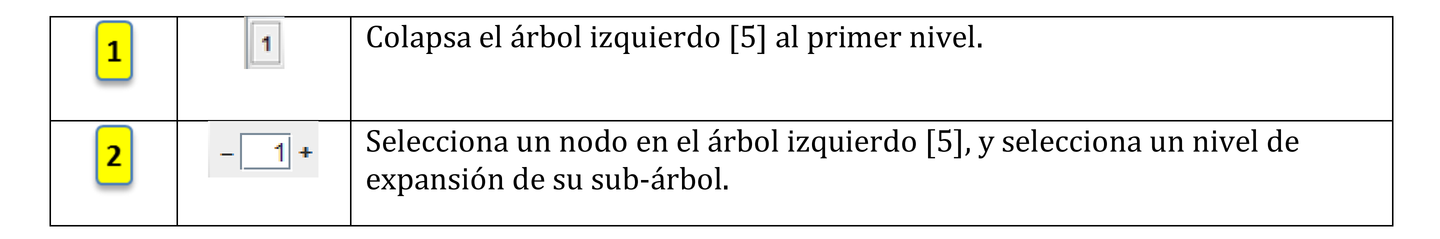
1		Clases de activos. Use el filtro [6] para acotar lo que se ve.
2		Amenazas. Use el filtro [7] para acotar lo que se ve.
3		Relación entre las clases de activos [1] y las amenazas [2] en blanco — sin relación Y — relacionadas ... — expandir para ver los detalles

		clase	sólo asociada a la clase indicada
4	1	Colapsa el árbol de clases de activos [1] al primer nivel de expansión	
5	– 1 +	Seleccione un nodo en [1], y seleccione un nivel de expansión de su sub-árbol.	
6		Filtro para clases de activos. Haga clic para seleccionar lo que quiere ver.	
7		Filtro para amenazas. Haga clic para seleccionar lo que quiere ver.	
8		Guardar el proyecto.	
9		Guardar y cerrar.	

5.3.4 comparación: clases / clases

Usted está editando TSV_1. Se presenta otro perfil TSV_2 para estudiar las diferencias.



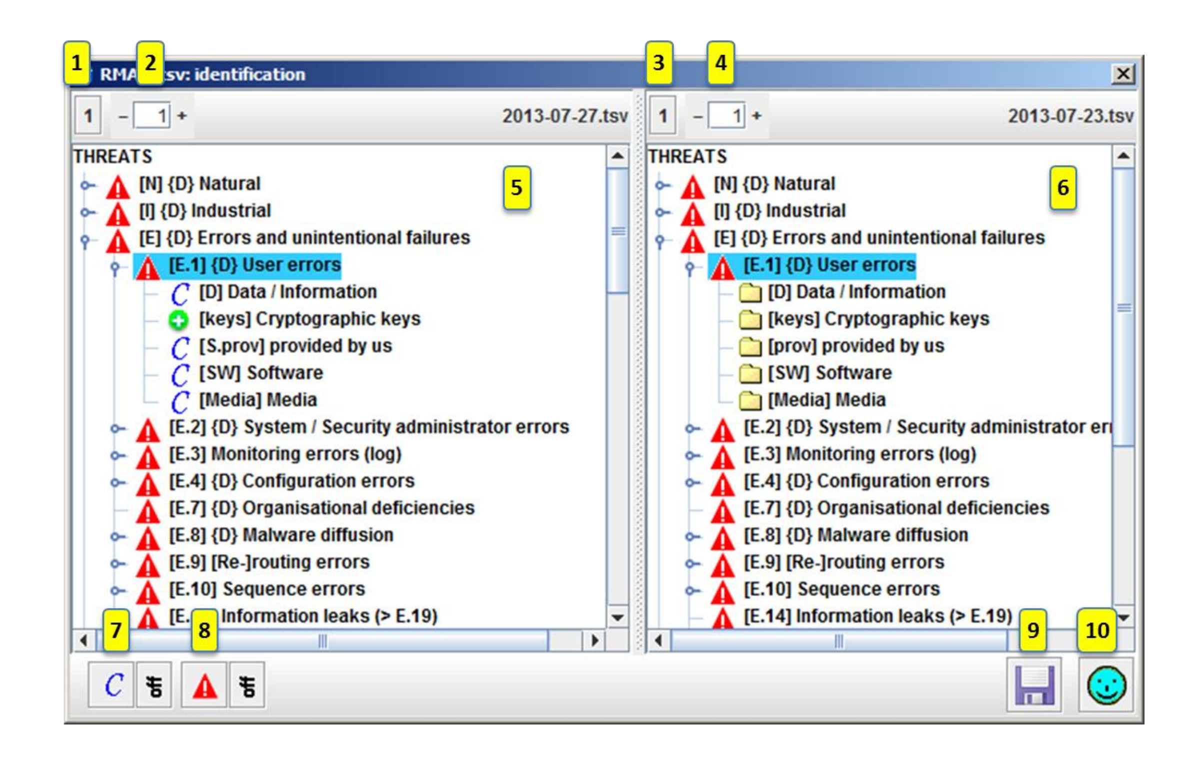


1	1	Colapsa el árbol izquierdo [5] al primer nivel.
2	– 1 +	Selecciona un nodo en el árbol izquierdo [5], y selecciona un nivel de expansión de su sub-árbol.

3	1	Colapsa el árbol derecho [6] al primer nivel.
4	– 1 +	Selecciona un nodo en el árbol derecho [6], y selecciona un nivel de expansión de su sub-árbol.
5		TSV_1, el que estamos editando ... (carpetas): grupo de clases de activos C: una clase de activos (triángulo rojo): una amenaza que está presente tanto en TSV_1 como en TSV_2 haga clic para eliminarla de TSV_1 (signo más verde): una amenaza que está presente en TSV_2, pero no en TSV1 haga clic para añadirla a TSV_1 (signo menos rojo): una amenaza que está presente en TSV_1, pero no en TSV2 haga clic para eliminarla de TSV_1
6		TSV_2, el árbol contra el que nos estamos comparando
7	C	Filtro para clases de activos. Haga clic para seleccionar lo que quiere ver.
8		Filtro para amenazas. Haga clic para seleccionar lo que quiere ver.
9		Guardar el proyecto.
10		Guardar y cerrar.

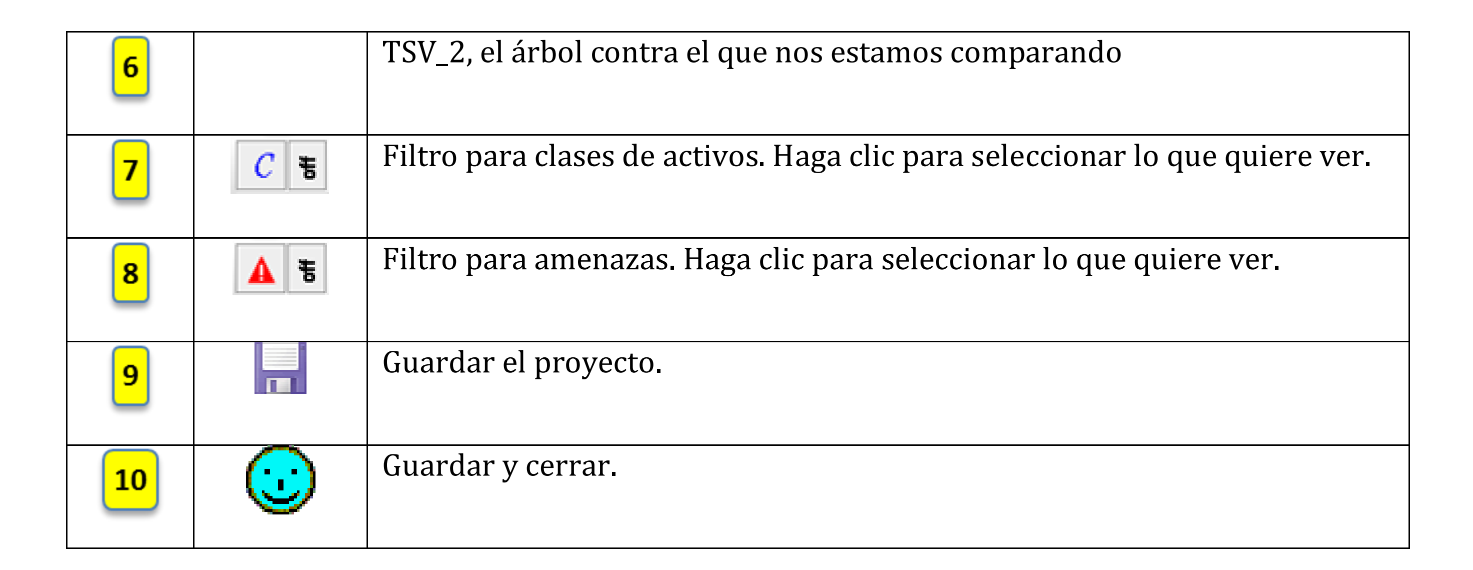
5.3.5 comparación: amenazas / amenazas

Usted está editando TSV_1. Se presenta otro perfil TSV_2 para estudiar las diferencias.



1	1	Colapsa el árbol izquierdo [5] al primer nivel.
2	– 1 +	Selecciona un nodo en el árbol izquierdo [5], y selecciona un nivel de expansión de su sub-árbol.
3	1	Colapsa el árbol derecho [6] al primer nivel.
4	– 1 +	Selecciona un nodo en el árbol derecho [6], y selecciona un nivel de expansión de su sub-árbol.
5		TSV_1, el que estamos editando …

	grupo de clases de activos
	una amenaza
C	una clase de activos presente en TSV_1 y en TSV_2 haga clic para eliminarla de TSV_1
	una clase de activos que está presente en TSV_2, pero no en TSV1 haga clic para añadirla a TSV_1
	una clase de activos que está presente en TSV_1, pero no en TSV2 haga clic para eliminarla de TSV_1



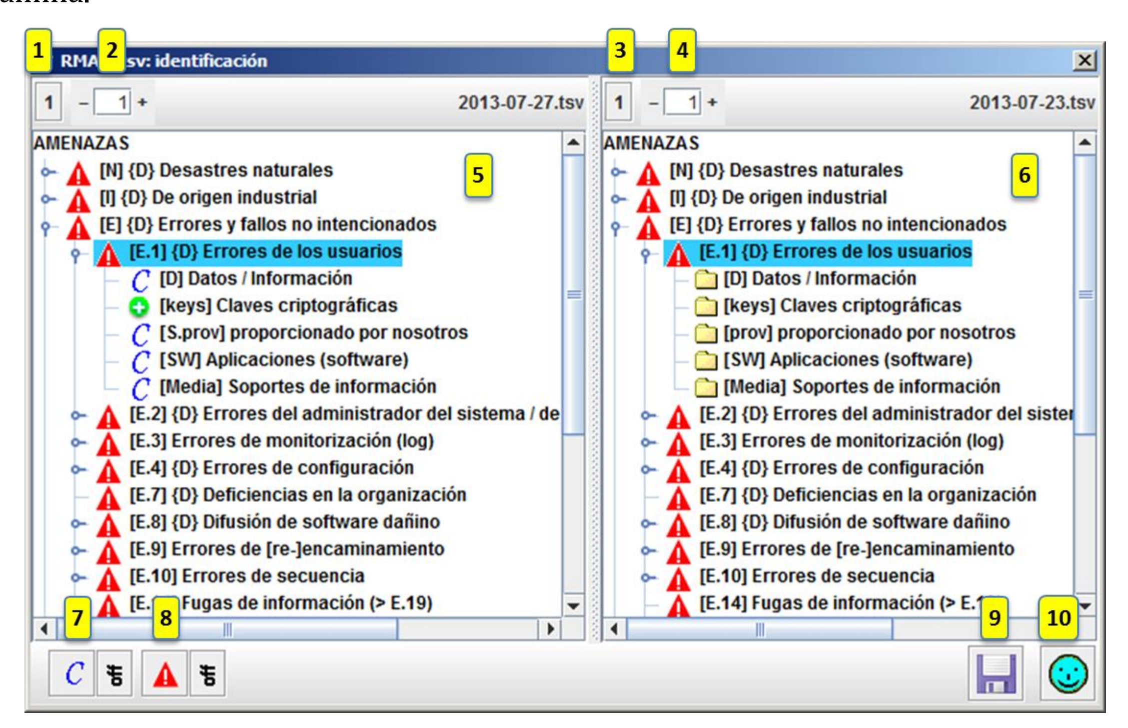
6		TSV_2, el árbol contra el que nos estamos comparando
7		Filtro para clases de activos. Haga clic para seleccionar lo que quiere ver.
8		Filtro para amenazas. Haga clic para seleccionar lo que quiere ver.
9		Guardar el proyecto.
10		Guardar y cerrar.

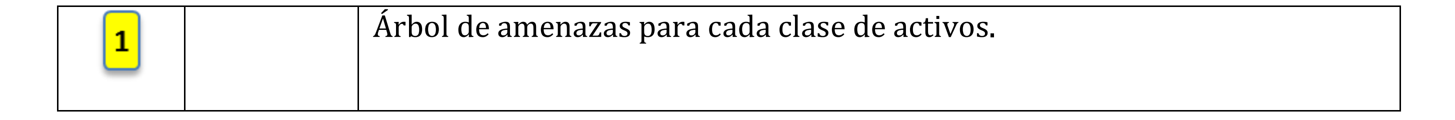
5.4 Valoración

Para asignar valores a las estimaciones de probabilidad y degradación de las amenazas asociadas a cada familia.

5.4.1 Amenazas por clase de activos

Para asignar valores a las estimaciones de probabilidad y degradación de las amenazas asociadas a cada familia.





1		Árbol de amenazas para cada clase de activos.

2		Probabilidad, medida como frecuencia anual. (ARO – Annual Rate of Occurrence)
3		Interrupción del servicio. Tiempo estimado que tardará el servicio en recuperarse tras una ocurrencia de la amenaza.
4		Dimensiones de seguridad. Estimación de la degradación: 0% - 100%.
5		Valores para la probabilidad [2], interrupción del servicio [3] y degradación en cada dimensión [4]. RMAT tiene conocimiento interno del tipo de amenaza y ls dimensiones de seguridad afectadas. Cuando RMAT piensa que una dimensión no está afectada, la celda se pone gris. Puede obviar esta opinión y establecer el valor que crea más oportuno. Cuando el valor no es explícito, sino heredado de la clase anfitriona, el valor se muestra entre llaves cuadradas.
6	1	Colapsa el árbol [1] al primer nivel.
7	– 1 +	Seleccione un nodo en el árbol [1], y el nivel de expansión de su sub-árbol
8	C	Filtro de clases de activos. Haga clic para seleccionar qué activos quiere ver.
9		Filtro de amenazas. Haga clic para seleccionar qué amenazas quiere ver.
10		Deshace la última asignación.
11		Vuelve a ejecutar el último deshacer..
12	CSV	Exporta a CSV
13		Guardar el proyecto.
14		Guardar y cerrar.

Expanda el árbol hasta que encuentre la clase de activos que busca. Las amenazas asociadas aparecen debajo.

Para cada amenaza puede establecer la probabilidad de ocurrencia, el intervalo de interrupción del servicio y la degradación en cada dimensión de seguridad.

Algunas celdas aparecen sombreadas. Eso significa que RMAT piensa que la amenaza no afecta a esa dimensión. En cualquier caso, si disiente de RMAT e ingresa un valor, ese valor será el que use PILAR.

Si selecciona una amenaza y hace clic con el botón derecho, aparecen varias opciones:

eliminar

disocia la amenaza de la clase de activos

push down: copiar la amenaza en los hijos

la amenaza se copia en todos y cada un de los hijos; si es nueva, se copian los valores de probabilidad y degradación

copy down: copiar los valores de la amenaza en los hijos

los valores se copian a los hijos que tengan asociada dicha amenaza

push up: copiar la amenaza en el padre

la amenaza se copia al padre; los valores se copian si la amenaza es nueva

copy up: copiar los valores de la amenaza en el padre

los valores se copian del hijo al padre, si este también tiene la amenaza asociada

Para guardar los datos actuales

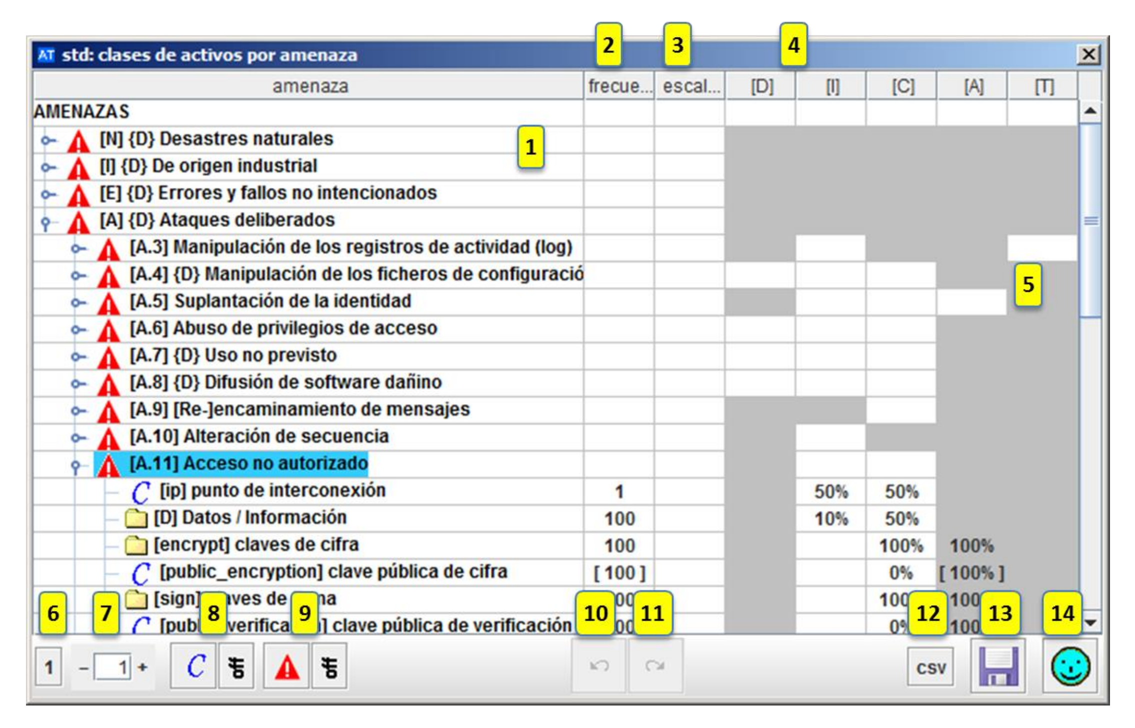
1. haga clic en GUARDAR

Para cerrar la ventana guardando los datos,

1. haga clic en OK

5.4.2 Clases de activos por amenaza

Para asignar valores a las estimaciones de probabilidad y degradación de las clases asociadas a cada amenaza.



1		Árbol de clases por cada amenaza.
2		Probabilidad, medida como frecuencia anual. (ARO – Annual Rate of Occurrence)
3		Interrupción del servicio. Tiempo estimado que tardará el servicio en recuperarse tras una ocurrencia de la amenaza.
4		Dimensiones de seguridad. Estimación de la degradación: 0% - 100%.
5		Valores para la probabilidad [2], interrupción del servicio [3] y degradación en cada dimensión [4]. RMAT tiene conocimiento interno del tipo de amenaza y ls dimensiones de seguridad afectadas. Cuando RMAT piensa que una dimensión no está afectada, la celda se pone gris. Puede obviar esta opinión y establecer el valor que crea más oportuno. Cuando el valor no es explícito, sino heredado de la clase anfitriona, el valor se muestra entre llaves cuadradas.
6	1	Colapsa el árbol [1] al primer nivel.
7	- 1 +	Seleccione un nodo en el árbol [1], y el nivel de expansión de su sub-árbol
8	C	Filtro de clases de activos. Haga clic para seleccionar qué activos quiere ver.
9		Filtro de amenazas. Haga clic para seleccionar qué amenazas quiere ver.
10		Deshace la última asignación.
11		Vuelve a ejecutar el último deshacer..
12	CSV	Exporta a CSV
13		Guardar el proyecto.
14		Guardar y cerrar.

Expanda el árbol hasta que encuentre la amenaza que busca. Las clases asociadas aparecen debajo.

Para cada clase puede establecer la probabilidad de ocurrencia, el intervalo de interrupción del servicio y la degradación en cada dimensión de seguridad.

Algunas celdas aparecen sombreadas. Eso significa que RMAT piensa que la amenaza no afecta a esa dimensión. En cualquier caso, si disiente de RMAT e ingresa un valor, ese valor será el que use PILAR.

Si selecciona una clase y hace clic con el botón derecho, aparecen varias opciones:

eliminar

disocia la amenaza de la clase de activos

Para guardar los datos actuales

1. haga clic en GUARDAR

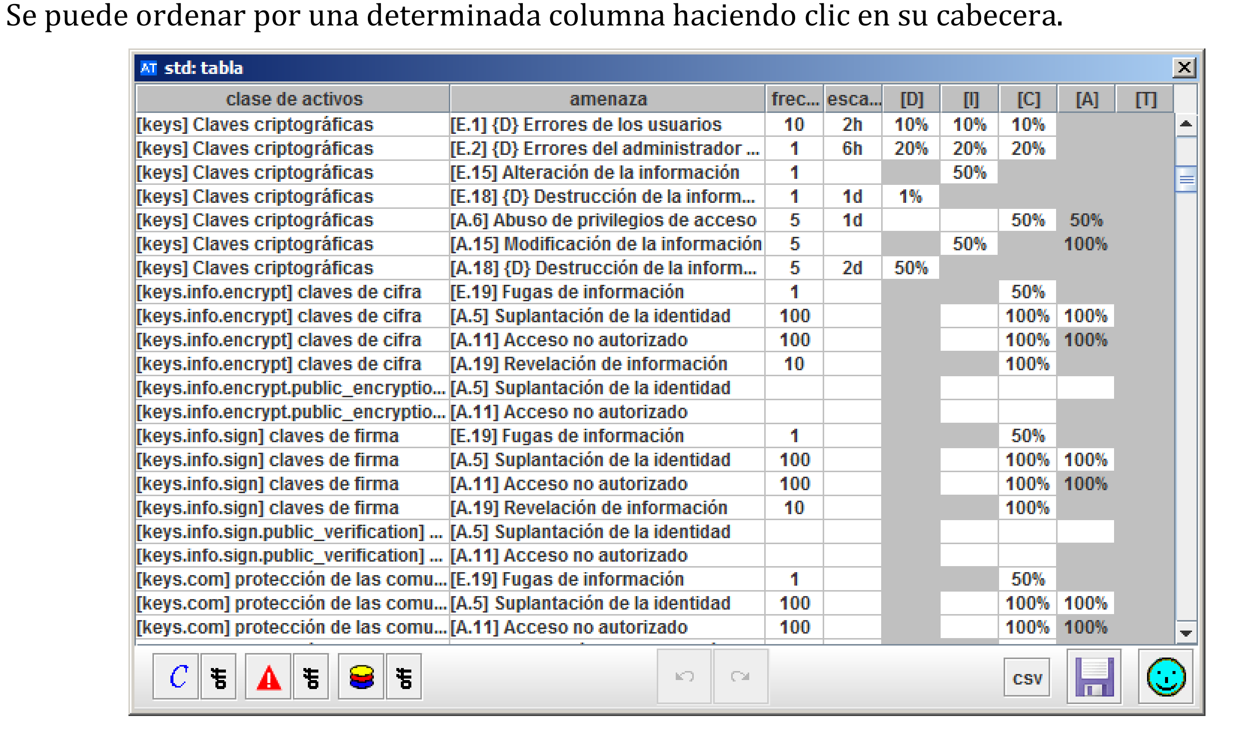
Para cerrar la ventana guardando los datos,

1. haga clic en OK

5.4.3 Tabla

Presentación plana de clases de activos, amenazas, probabilidades y valores de degradación.

Se puede ordenar por una determinada columna haciendo clic en su cabecera.

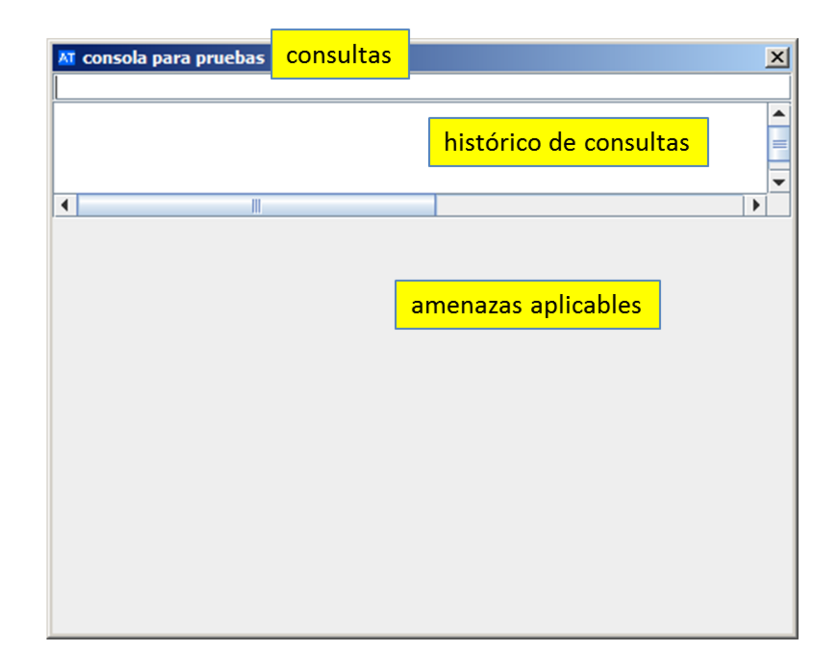

std: tabla

clase de activos	amenaza	frec...	esca...	[D]	[I]	[C]	[A]	[T]
[keys] Claves criptográficas	[E.1] {D} Errores de los usuarios	10	2h	10%	10%	10%		
[keys] Claves criptográficas	[E.2] {D} Errores del administrador ...	1	6h	20%	20%	20%		
[keys] Claves criptográficas	[E.15] Alteración de la información	1			50%			
[keys] Claves criptográficas	[E.18] {D} Destrucción de la inform...	1	1d	1%				
[keys] Claves criptográficas	[A.6] Abuso de privilegios de acceso	5	1d			50%	50%	
[keys] Claves criptográficas	[A.15] Modificación de la información	5			50%		100%	
[keys] Claves criptográficas	[A.18] {D} Destrucción de la inform...	5	2d	50%				
[keys.info.encrypt] claves de cifra	[E.19] Fugas de información	1				50%		
[keys.info.encrypt] claves de cifra	[A.5] Suplantación de la identidad	100				100%	100%	
[keys.info.encrypt] claves de cifra	[A.11] Acceso no autorizado	100				100%	100%	
[keys.info.encrypt] claves de cifra	[A.19] Revelación de información	10				100%		
[keys.info.encrypt.public_encryptio...	[A.5] Suplantación de la identidad							
[keys.info.encrypt.public_encryptio...	[A.11] Acceso no autorizado							
[keys.info.sign] claves de firma	[E.19] Fugas de información	1				50%		
[keys.info.sign] claves de firma	[A.5] Suplantación de la identidad	100				100%	100%	
[keys.info.sign] claves de firma	[A.11] Acceso no autorizado	100				100%	100%	
[keys.info.sign] claves de firma	[A.19] Revelación de información	10				100%		
[keys.info.sign.public_verification] ...	[A.5] Suplantación de la identidad							
[keys.info.sign.public_verification] ...	[A.11] Acceso no autorizado							
[keys.com] protección de las comu...	[E.19] Fugas de información	1				50%		
[keys.com] protección de las comu...	[A.5] Suplantación de la identidad	100				100%	100%	
[keys.com] protección de las comu...	[A.11] Acceso no autorizado	100				100%	100%	

5.5 Consola de pruebas

Permite indicar una clase de activos o una combinación de clases, para estudiar las amenazas que PILAR asignaría un activo con esa combinación.

La interfaz tiene 3 partes:

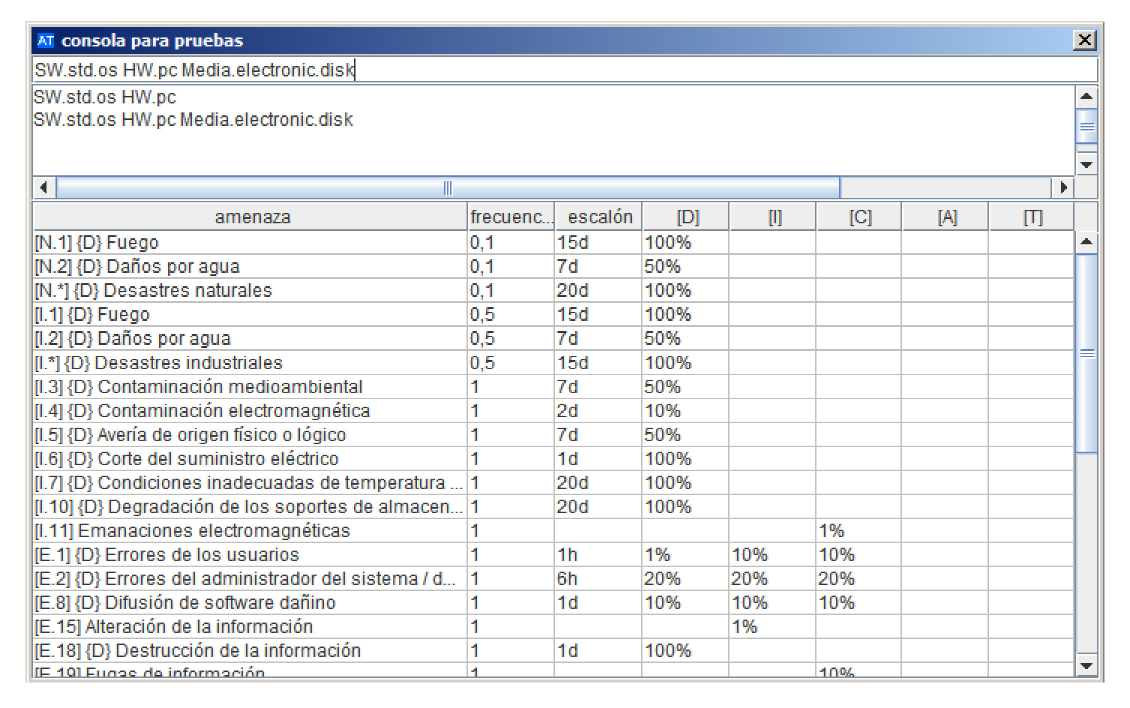


El primer panel es la pregunta: una o más clases de activos.

El segundo panel conserva la historia de preguntas. Esto facilita recodar lo que ha preguntado previamente e incluso repreguntar con alguna variación.

El tercer panel despliega las amenazas acumuladas sobre la combinación planteada en el primer panel.

Ejemplo:



amenaza	frecuenc...	escalón	[D]	[I]	[C]	[A]	[T]
[N.1] {D} Fuego	0,1	15d	100%				
[N.2] {D} Daños por agua	0,1	7d	50%				
[N.*] {D} Desastres naturales	0,1	20d	100%				
[I.1] {D} Fuego	0,5	15d	100%				
[I.2] {D} Daños por agua	0,5	7d	50%				
[I.*] {D} Desastres industriales	0,5	15d	100%				
[I.3] {D} Contaminación medioambiental	1	7d	50%				
[I.4] {D} Contaminación electromagnética	1	2d	10%				
[I.5] {D} Avería de origen físico o lógico	1	7d	50%				
[I.6] {D} Corte del suministro eléctrico	1	1d	100%				
[I.7] {D} Condiciones inadecuadas de temperatura ...	1	20d	100%				
[I.10] {D} Degradación de los soportes de almacen...	1	20d	100%				
[I.11] Emanaciones electromagnéticas	1				1%		
[E.1] {D} Errores de los usuarios	1	1h	1%	10%	10%		
[E.2] {D} Errores del administrador del sistema / d...	1	6h	20%	20%	20%		
[E.8] {D} Difusión de software dañino	1	1d	10%	10%	10%		
[E.15] Alteración de la información	1			1%			
[E.18] {D} Destrucción de la información	1	1d	100%				
[E.19] Fugas de información	1				10%		

6 Expresiones condicionales para controles y preguntas

RMAT usa expresiones condicionales para controles y preguntas: para saber si el control es de obligado cumplimiento (mandatory) y para saber si es aplicable o no.

Se usa una notación XML para introducir expresiones:

```
expression ::=
   | <and [ set ] > { expression }0+ </and>
   | <or [ set ] > { expression }0+ </or>
   | <true />
   | <false />
   | <var name />
   | <family set />
   | <under set />
   | <dimension set />
   | <threat set />
   | <value [ dimension ] [ range ] />
   | <risk [ dimension ] [ threat ] [ range ] />
```

Y se trata de saber si la expresión evalúa a CIERTO o FALSO en un dominio de seguridad dado.

<and>

Evalúa a CIERTO si todos los términos son CIERTOS. Si no, evalúa a FALSO. Cuando la fórmula incluye variables, los nombres pueden meterse en el atributo SET.

Ejemplo: <and set="CM" > <family set="COM" /> </and>
evalúa a CIERTO cuando CM es CIERTA y hay activos de la clase COM.

<or>

Evalúa a CIERTO si algún término es CIERTO. Si no, evalúa a FALSO. Cuando la fórmula incluye variables, los nombres pueden meterse en el atributo SET.

Ejemplo: <or set="CM, CH" > <family set="D.per" /> </or>
evalúa a CIERTO cuando CM es CIERTO, o CH es CIERTO, o hay activos de la clase D.per.

<true />

Evalúa a CIERTO.

<false />

Evalúa a FALSO.

<var name="x" />

Evalúa al valor de la variable "x" en el dominio de seguridad.

<family set="SW.std.os, HW.PC" />

Evalúa a CIERTO si el dominio de seguridad contiene al menos un activo de alguna de las clases indicadas.

<under set="D.classified.confidential, D.classified.restricted" />

Evalúa a CIERTO si el dominio de seguridad contiene al menos un activo de alguna de las clases indicadas o del qu depende algún activo de alguna de las clases indicadas.

<dimension set="C, I" />

Evalúa a CIERTO si el dominio contiene algún activo que es valioso en alguna de las dimensiones de seguridad indicadas.

<threat set=”E.14, A.14” />

Evalúa a CIERTO si el dominio contiene algún activo que está expuesto a alguna de las amenazas indicadas.

<value dimension=”C” range=”3-5” />

Evalúa a cierto si existe algún activo en el dominio cuyo valor en la dimensión indicada está en el rango indicado. Si no se indica la dimensión, basta que el valor en alguna dimensión esté en el rango indicado. Si no se indica rango, basta que el valor en la dimensión indicada sea mayor que 0.

<risk dimension=”C” threat=”A.14” range=”-5” />

PILAR analiza todos los riesgos para todos los activos en el dominio de seguridad. Filtra aquellos que casan con alguna de las dimensiones, si es que se indican. Filtra aquellos que casan con las amenazas que se citan. La condición evalúa a CIERTO si el riesgo está en el rango indicado. Si no se indica rango de riesgo, se evalúa a CIERTO si el nivel de riesgo es mayor que {0}.

6.1 Rangos de riesgo

Un rango es un intervalo

- **a-b (entre)**

  a <= riesgo y riesgo <= b

- **-b** (hasta …)

  riesgo <= b

- **a- (a partir de …)**

  a <= riesgo

6.2 Definición of variables

En la raíz del perfil se pueden definir variables booleanas-

Ejemplos:

```
<define name="CH">
  <value dimension="C " range="(6-)" />
</define>
<define name="CM">
  <value dimension="C " range="(3-)" />
</define>
<define name="CL">
  <value dimension="C " range="(1-)" />
</define>
```

7 Expresiones condicionales para medidas de protección (KB)

RMAT usa expresiones condicionales para establecer si una medida de protección es útil para mitigar un cierto riesgo.

Las expresiones se escriben usando un formato XML:

```
expression ::=
      <and> { expression }0+ </and>
      | <or> { expression }0+ </or>
      | <term [F] [S] [D] [C] [V] [Z] [R] [M] [only] />
```

Básicamente, un TERM describe los parámetros que identifican un riesgo al que la medida se puede aplicar. Puede definir varias combinaciones por medio de expresiones <OR>, o puede requerir varias condiciones por medio de expresiones <AND>.

Un término describe un patrón para filtrar riesgos:

- un activo
- una amenaza
- una dimensión de seguridad
- un nivel de riesgo

F="class, class, ..."

Si el activo es de alguna de las clases indicadas.

S="class, class, ..."

Si el activo X tiene algún otro activo A que depende de X, y A es de alguna de las clases indicadas.

D="dimension, dimension, ..."

Si la dimensión afectada está en la lista.

C="criterion, criterion, ..."

Si alguno de los criterios de valoración del activo está en la lista.

V="value"

Z="threat, threat, ..."

Si la amenaza está en la lista.

only="true or false"

CIERTO si la medida es útil únicamente para lo que se marca explícitamente.

R="range"

Si el riesgo está en el rango. Un rango es un intervalo

- **a-b (entre)**

  a <= riesgo y riesgo <= b

- **-b** (hasta ...)

  riesgo <= b

- **a- (a partir de ...)**

a <= riesgo

M="mode, mode, ..."

Si el modo de operación del sistema está en la lista.

8 Instalación

Instale PILAR antes de instalar RMAT. RMAT usa los ficheros de configuración de PILAR.

8.1 Windows

- ejecute rmat_<version>_lang.exe
- siga las instrucciones para instalarlo en el directorio que guste
  - varios idiomas pueden compartir directorio
  - varias versiones pueden requerir varios directorios
  - sugerencia: C:Archivos de Programa</w:t>RMAT_version
- al terminar la instalación, tendrá un fichero de nombre
  rmat.exe
  en el directorio de instalación.

Los términos de uso de la herramienta se mostrarán al ejecutarla.

8.2 UNIX, Linux

- ejecute rmat_linux_<version>_lang.jar
- siga las instrucciones para instalarlo en el directorio que guste
  - varios idiomas pueden compartir directorio
  - varias versiones pueden requerir varios directorios
  - sugerencia:
    - /usr/local/bin
    - /usr/local/lib/RMAT_version
- al terminar la instalación, tendrá un fichero de nombre
  rmat.jar
  en el directorio de instalación.

Los términos de uso de la herramienta se mostrarán al ejecutarla.

8.3 Mac OSX

- ejecute rmat_mac_<version>_lang.jar
- siga las instrucciones para instalarlo en el directorio que guste
  - varios idiomas pueden compartir directorio
  - varias versiones pueden requerir varios directorios
  - sugerencia:
    - /Applications
    - ~usuario/Library/RMAT_version
- al terminar la instalación, tendrá un fichero de nombre
  rmat.app
  en el directorio de instalación.

Los términos de uso de la herramienta se mostrarán al ejecutarla.